NASA Integrated Communications Services (NICS)

Attachment C Background and Historical

DRAFT

23 April 2009

Table of Contents

1 NICS BACKGROUND AND HISTORICAL 19
1.1 DISCLAIMER 19
1.2 NASA IT OVERVIEW 19
1.3 IT INFRASTRUCTURE IMPROVEMENT PROGRAM (I^3P) 19
1.3.1 Enterprise Service Desk (ESD) (Tier 1) 21
1.3.2 Enterprise Service Request System (ESRS) 21
1.3.3 NASA Enterprise Data Center (NEDC) 21
1.3.4 Agency Consolidated End-User Services (ACES) 21
1.3.5 Enterprise Application Service Technology (EAST) 22
1.3.6 Web Enterprise Service Technology (WEST) 22
1.4 NICS COORDINATION WITH CENTER INFORMATION OFFICES (CIO) 22
1.4.1 Coordination with MSFC IT Services (MITS) 22
1.4.2 Coordination with Center CIOs 23
1.5 NICS OVERVIEW 23
1.5.1 Existing NASA Contracts that Become Part of NICS 23
1.5.2 Tours of Duty 26
1.5.3 NICS Location of Performance: 26
1.6 DOCUMENT OVERVIEW 27
1.7 APPLICABLE DOCUMENTS 28

2 UNITeS CONTRACT MANAGEMENT 29
2.1 UNITeS PROGRAM MANAGEMENT 31
2.1.1 UNITeS Risk Management 31
2.2 UNITeS FINANCIAL MANAGEMENT 31
2.2.1 UNITeS Management Information Control System (MICS) 31
2.2.2 UNITeS Integrated Enterprise Financial (IEF) 34
2.2.3 UNITeS OMB Circular A-11, Exhibit 300 34
2.3 UNITeS LOGISTICS 34
2.3.1 UNITeS Property/Inventory Management 35
2.3.2 UNITeS Shipping/Receiving/Inspection Services 35
2.3.3 UNITeS Vehicles 36
2.4 UNITeS PROCUREMENT 38
2.5 UNITeS SECURITY MANAGEMENT 39
2.5.1 UNITeS Physical Security 39
2.5.2 UNITeS Information Technology (IT) Security 39
2.5.3 UNITeS Export Control 40
2.5.4 UNITeS Emergency Management 40

2.6 UNITeS SAFETY, HEALTH, AND ENVIRONMENTAl (SHE) MANAGEMENT....42
2.6.1 UNITeS Safety....42
2.6.2 UNITeS Safety Performance....43
2.7 UNITeS FACILITIES MANAGEMENT....44
2.8 UNITeS QUALITY ASSURANCE AND MANAGEMENT....45
2.9 UNITeS CONTRACT AND SUBCONTRACT ADMINISTRATION....45
2.9.1 UNITeS Subcontracts in Support of NISN....46
2.10 UNITeS WORK LOAD INDICATORS....47
2.10.1 UNITeS Contract Direct Hours....47
2.10.2 UNITeS Office Supplies....47
2.11 APPLICABLE DOCUMENTS....48

3 UNITeS NISN ENTERPRISE SERVICES....51
3.1 UNITES NISN CORPORATE NETWORK SERVICES....51
3.1.1 UNITeS NISN Internet Protocol Address Management (IPAM)....52
3.1.1.1 UNITeS NISN IPAM Migration (IPAM) Project....52
3.1.2 UNITeS NISN Remote Access Services (RAS)....52
3.1.3 UNITeS NISN Network Timing Protocol (NTP) Service....53
3.1.4 UNITeS NISN Guest Network Services....53
3.2 UNITES NISN CORPORATE VOICE SERVICES....53
3.3 RESERVED....53
3.4 UNITES NISN CORPORATE DATA SERVICES....54
3.4.1 UNITeS NISN Corporate Routed Data....54
3.4.1.1 Routed Data Class of Service....59
3.4.1.2 WANX Project....61
3.4.1.3 Corporate Routed Data Peering....64
3.4.1.4 Corporate Routed Data IPv6....66
3.4.2 UNITeS NISN Data Center Networks....69
3.4.2.1 Layer 3 VPN (L3VPN)....70
3.4.3 UNITeS NISN Custom Networks....70
3.4.3.1 International Networks....71
3.4.3.2 DRFC Infrastructure Support....71
3.4.3.3 Multi Channel Digital Television (MCDTV)....72
3.4.4 UNITeS NISN Firewall Services....74
3.4.5 UNITeS NISN Proxy Services....74
3.4.6 Reserved....74
3.4.7 UNITeS NISN Layer 2 VPN Services....75
3.4.8 UNITeS NISN International Services....75
3.5 UNITES NISN CORPORATE COLLABORATION SERVICES....77
3.5.1 UNITeS NISN Video Conferencing Service (VCS)....77

3.5.1.1 NISN VCS Enterprise Infrastructure 77
3.5.1.2 NISN VCS Room Packages 78
3.5.1.3 NISN VCS Reservation System 79
3.5.2 UNITeS NISN Audio Conferencing Service (ACS) 80
3.5.3 Reserved 80
3.6 UNITES NISN CORPORATE MANAGEMENT AND OPERATIONS 80
3.6.1 UNITeS NISN Corporate Network Management and Monitoring 80
3.6.2 Colaboration Management and Monitoring 81
3.6.2.1 Collaboration NASA Teleconferencing Center 81
3.6.2.2 Collaboration Maintenance 82
3.6.2.3 UNITeS NTC Coordinate with GSA 83
3.6.2.4 UNITeS NTC/GSA Provided Conference Reservation System 84
3.6.2.5 VCS Room Operator 84
3.6.3 UNITeS NISN Technical Field Support 85
3.6.3.1 NISN Clearances Needed for Gateways and ENMC 85
3.6.4 UNITeS NISN Corporate Maintenance 85
3.6.5 UNITeS NISN Corporate Services Scheduling 85
3.6.5.1 NISN Corporate Freeze Policy 85
3.6.6 UNITeS NISN Tier 2 Service Desk Management and Integration 85
3.7 UNITES/MOMS NISN MISSION SERVICES 86
3.7.1 NISN UNITeS/ MOMS Mission Voice Services 87
3.7.2 UNITeS NISN/MOMS Mission Video Services 88
3.7.3 UNITES NISN/MOMS Mission Routed Data Services 90
3.7.4 UNITeS NISN/MOMS MISSION Integration Services 91
3.7.4.1 Mission Communications Manager 91
3.7.4.2 Communications Manager 92
3.7.5 UNITeS NISN/MOMS Mission Dedicated Data and Custom Services92
3.7.5.1 Mission Software Development 93
3.7.6 UNITeS NISN/MOMS Center-Specific Mission Services 94
3.7.7 UNITeS Mission IT Security Services 94
3.7.8 UNITeS NISN/MOMS Mission Configuration Management and Documentation 95
3.8 UNITES NISN/MOMS MISSION MANAGEMENT AND OPERATIONS 95
3.8.1 UNITeS NISN/MOMS Communications Control 95
3.8.1.1 Operations Centers 97
3.8.1.2 Mission Operations Clearances 97
3.8.2 UNITeS NISN/MOMS Installation and Maintenance 97
3.8.3 UNITeS NISN/MOMS Network Scheduling 98
3.8.3.1 Mission Freezes 99
3.8.4 UNITeS NISN/MOMS Mission IT Security Operations Support 99

3.8.4.1 Mission IT Security Operations 99
3.8.4.2 Mission Security Control Center 100
3.8.5 UNITeS NISN/MOMS Mission Facilities Management 100
3.9 UNITES NISN CUSTOMER RELATIONSHIP MANAGEMENT 100
3.9.1 UNITeS NISN Customer Service Representatives (CSRs) 101
3.10 UNITES NISN SERVICE MANAGEMENT 102
3.10.1 UNITeS NISN Facilities Engineering 102
3.10.2 UNITeS NISN Service Delivery Support Software 102
3.10.2.1 NISN Service Requests 102
3.10.3 UNITeS NISN Configuration Management 102
3.11 UNITES NISN STRATEGY GENERATION 103
3.11.1 UNITeS NISN Strategic Planning 104
3.11.2 UNITeS NISN Support to the Enterprise Architecture 104
3.11.3 UNITeS NISN Corporate Network Capacity Planning 104
3.11.4 UNITeS NISN Network Modeling 104
3.12 UNITES NISN IT SECURITY SERVICES 107
3.12.1 UNITeS NISN /Incident Response 107
3.12.2 UNITeS NISN IT Security Perimeter 107
3.12.3 UNITeS NISN Security Operations 108
3.12.3.1 NISN Clearances Needed for Security Operations 109
3.13 UNITES NISN GSA CONTRACT INTEGRATION 109
3.13.1 GSA CONTRACT INTEGRATION 109
3.13.1.1 Additional GSA Workload Actions 112
3.13.1.2 Purchased Telecommunications Services 112
3.14 UNITES NISN/MOMS WORK LOAD INDICATORS 112
3.14.1 UNITeS NISN Corporate Work Load Indicators 112
3.14.1.1 Contract Direct Hours 112
3.14.1.2 Corporate Network Trouble Tickets 113
3.14.1.3 Corporate Purchase Orders 113
3.14.1.4 Corporate Network Vendor Maintenance 113
3.14.1.5 NISN User Training 113
3.14.2 UNITeS NISN/MOMS Mission Work Load Indicators 113
3.14.2.1 Mission Direct Hours 113
3.14.2.2 Mission Trouble Tickets 114
3.14.2.3 Mission Network Vendor Maintenance 114
3.14.3 NISN UNITeS Mission and Corporate Network Service Request 114
3.15 APPLICABLE DOCUMENTS 114

4 CENTER AND ASSOCIATED COMPONENT FACILITY SERVICES 118
4.1 AMES RESEARCH CENTER (ARC) 118

4.1.1 Property/Inventory 118
4.1.2 Shipping/Receiving/Inspection 118
4.1.3 Vehicles Necessary To Support Center Work 118
4.1.4 Physical Security 118
4.1.5 Emergency Management 118
4.1.6 Safety 118
4.1.7 Facilities 118
4.1.8 Network Services 119
4.1.8.1 IPAM 119
4.1.8.2 RAS 119
4.1.8.3 NTP 119
4.1.8.4 Guest Network 120
4.1.9 Data Services 120
4.1.9.1 High Level LAN Description 120
4.1.9.2 Wireless Networks 122
4.1.9.3 Network Security 123
4.1.9.4 Network Operations 123
4.1.9.5 Network Processes 123
4.1.9.6 Network Lab 123
4.1.9.7 Hardware Description 124
4.1.9.8 Hardware Refresh 124
4.1.10 Collaboration Services 124
4.1.11 Customer Relationship Management 124
4.1.12 IT Security 124
4.1.13 Cable Plant Services 124
4.1.13.1 Optical Fiber 124
4.1.13.2 Twisted Pair Copper Cabling 125
4.1.14 Emergency Warning Systems (RESERVED) 125
4.1.15 Public Address Systems 125
4.1.16 Radio Services 125
4.1.16.1 Centerwide Trunking Radio Infrastructure 125
4.1.16.2 T-Radio System Technical Requirements 126
4.1.17 Telephone Services 127
4.1.17.1 Number of Trunks 127
4.1.17.2 Call Processing 127
4.1.17.3 Voice Mail Services 127
4.1.17.4 E911 Services 128
4.1.17.5 Analog Phone and FAX Services 128
4.1.18 Voice over Internet Protocol (VoIP) (RESERVED) 128
4.1.19 Cable Television Services 128
4.1.20 Continuation of Center Zoned Architecture Project (CZAP) 128

4.1.21 Ongoing Center-Specific Projects 128
4.1.22 Work Load Indicators 128
4.1.23 Applicable Documents 129
4.2 DRYDEN FLIGHT RESEARCH CENTER (DFRC) 130
4.2.1 Property/Inventory 130
4.2.2 Shipping/Receiving/Inspection 130
4.2.3 Vehicles Necessary To Support Center Work 130
4.2.4 Physical Safety 130
4.2.5 Emergency Management 130
4.2.6 Safety 130
4.2.7 Facilities 130
4.2.8 Network Services 131
4.2.8.1 IPAM 131
4.2.8.2 Remote Access 131
4.2.8.3 NTP 131
4.2.8.4 Guest Network Services 131
4.2.9 Data Services 131
4.2.9.1 High Level LAN Description 131
4.2.9.2 Wireless Networks 133
4.2.9.3 Network Security 134
4.2.9.4 Network Operations 135
4.2.9.5 Network Processes 135
4.2.9.6 Network Lab 135
4.2.9.7 Hardware Description 135
4.2.9.8 Hardware Refresh 137
4.2.10 Collaboration Services 137
4.2.10.1 ViTs Rooms 137
4.2.10.2 Conference Room Support 137
4.2.11 Customer Relationship Management 137
4.2.12 IT Security 137
4.2.13 Cable Plant Services (RESERVED) 137
4.2.14 Emergency Warning Systems (RESERVED) 138
4.2.15 Public Address System (RESERVED) 138
4.2.16 Radio Services (RESERVED) 138
4.2.17 Telephone Services (RESERVED) 138
4.2.18 Voice over Internet Protocol (VoIP) (RESERVED) 138
4.2.19 Cable Television Services (RESERVED) 138
4.2.20 Continuation of Center Zoned Architecture Project (CZAP) 138
4.2.21 Ongoing Center-Specific Projects 138
4.2.21.1 Dryden Data Center 138
4.2.22 Work Load Indicators 138

4.2.23 Applicable Documents 139
4.3 GLENN RESEARCH CENTER (GRC) 140
4.3.1 Property/Inventory 140
4.3.2 Shipping/Receiving/Inspection 140
4.3.3 Vehicles Necessary To Support Center Work 140
4.3.4 Physcial Security 141
4.3.5 Emergency Management 141
4.3.5.1 Center Specific COOP Support 141
4.3.5.2 Service Continuity of Operations Support 142
4.3.6 Safety 142
4.3.7 Facilities 142
4.3.8 Network Services 143
4.3.8.1 IPAM 143
4.3.8.2 RAS 143
4.3.8.3 NTP 144
4.3.8.4 Guest Network 144
4.3.9 Data Services 144
4.3.9.1 High Level LAN Description 144
4.3.9.2 Wireless Networks 145
4.3.9.3 Network Security 145
4.3.9.4 Network Operations 145
4.3.9.5 Network Processes 146
4.3.9.6 Network Lab 146
4.3.9.7 Hardware Description 146
4.3.9.8 Hardware Refresh 146
4.3.10 Collaboration Services 146
4.3.11 Customer Relationship Management (CRM) 146
4.3.12 IT Security 147
4.3.13 Cable Plant Services 147
4.3.13.1 Optical Fiber 149
4.3.13.2 Twisted Pair Copper Cabling 149
4.3.14 Emergency Warning System (RESERVED) 149
4.3.15 Public Address Systems (RESERVED) 149
4.3.16 Radio Services 149
4.3.17 Telephone Services 150
4.3.17.1 Handsets 150
4.3.17.2 Voice Mail Services 151
4.3.17.3 E911 Services 151
4.3.17.4 Trunks 151
4.3.18 Voice over Internet Protocol (VoIP) (RESERVED) 152
4.3.19 Cable Television Services 152

4.3.20 Continuation of Center Zoned Architecture Project (CZAP) 153
4.3.21 Ongoing Center-Specific Projects.....153
4.3.21.1 GRC Network Upgrade Completion.....153
4.3.21.2 GRC WAN Gateway Relocation 153
4.3.21.3 Telephone Service Replacement at GRC Lewis Field and Plum Brook 154
4.3.21.4 GRC Video Distribution System Redesign and Replacement.....154
4.3.21.5 Plum Brook Station Network Redesign and Replacement154
4.3.21.6 Construction Projects 154
4.3.22 Work Load Indicators 155
4.3.23 Applicable Documents 155
4.4 GODDARD SPACE FLIGHT CENTER (GSFC).....156
4.4.1 Property/Inventory 156
4.4.2 Shipping/Receiving/Inspection 156
4.4.3 Vehicles Necessary To Support Center Work 156
4.4.4 Physical Security.....156
4.4.5 Emergency Management.....156
4.4.6 Safety 156
4.4.7 Facilities 156
4.4.8 Network Services 157
4.4.8.1 IPAM.....157
4.4.8.2 RAS.....157
4.4.8.3 NTP 157
4.4.8.4 Guest Network 157
4.4.9 Data Services.....157
4.4.9.1 High Level LAN Description.....157
4.4.9.2 Wireless Networks 158
4.4.9.3 Network Security 158
4.4.9.4 Network Operations 158
4.4.9.5 Network Processes 161
4.4.9.6 Network Lab 161
4.4.9.7 Hardware Description 161
4.4.9.8 Hardware Refresh 163
4.4.10 Collaboration Services 163
4.4.11 Customer Relationship Management 163
4.4.12 IT Security.....163
4.4.13 Cable Plant Services (RESERVED) 163
4.4.14 Emergency Warning Systems (RESERVED).....163
4.4.15 Public Address Systems (RESERVED).....163
4.4.16 Radio Services (RESERVED) 163

4.4.17 Telephone Services (RESERVED) 163
4.4.18 Voice over Internet Protocol (VoIP) (RESERVED) 163
4.4.19 Cable Television Services (RESERVED) 163
4.4.20 Continuation of Center Zoned Architecture Project (CZAP) 164
4.4.21 Ongoing Center-Specific Projects 164
4.4.21.1 Space Science Building #34 IT Upgrade 164
4.4.21.2 CNE IT Upgrade 164
4.4.22 Work Load Indicators 164
4.4.23 Applicable Documents 164
4.5 NASA HEADQUARTERS (HQ) 165
4.5.1 Property/Inventory 165
4.5.2 Shipping/Receiving/Inspection 166
4.5.3 Vehicles Necessary To Support Center Work 166
4.5.4 Physical Security 166
4.5.5 Emergency Management 166
4.5.6 Safety 166
4.5.7 Facilities 166
4.5.8 Network Services 167
4.5.8.1 IPAM 167
4.5.8.2 RAS 167
4.5.8.3 NTP 167
4.5.8.4 Guest Network 167
4.5.9 Data Services 167
4.5.9.1 High Level LAN Description 168
4.5.9.2 Wireless Networks 169
4.5.9.3 Network Security 169
4.5.9.4 Network Operations 169
4.5.9.5 Network Processes 170
4.5.9.6 Network Lab 170
4.5.9.7 Hardware Description 170
4.5.9.8 Hardware Refresh 170
4.5.10 Colloaboration Services 170
4.5.11 Customer Relationship Management 171
4.5.12 IT Security 171
4.5.13 Cable Plant Services 171
4.5.14 Emergency Warning System 171
4.5.15 Public Address System 171
4.5.16 Radio Services (RESERVED) 172
4.5.17 Telephone Services (RESERVED) 172
4.5.18 Voice over Internet Protocol (VoIP) 172
4.5.19 Cable Television Services 173

4.5.20 Continuation of Center Zoned Architecture Project (CZAP) 173
4.5.21 Ongoing Center-Specific Projects.....173
4.5.22 Workload Indicators.....173
4.5.23 Applicable Documents.....173
4.6 JET PROPULSION LABORATORY (JPL) (RESERVED).....174
4.7 JOHNSON SPACE FLIGHT CENTER (JSC).....175
4.7.1 Property/Inventory 177
4.7.2 Shipping/Receiving/Inspection 177
4.7.3 Vehicles Necessary To Support Center Work 178
4.7.4 Physical Security.....178
4.7.5 Emergency Management.....178
4.7.6 Safety 178
4.7.7 Facilities 178
4.7.8 Network Services 179
4.7.8.1 IPAM.....180
4.7.8.2 Remote Access Services (RAS).....180
4.7.8.3 NTP 180
4.7.8.4 Guest Network 180
4.7.9 Data Services.....181
4.7.9.1 High Level LAN Description.....181
4.7.9.2 Wireless Networks.....182
4.7.9.3 Network Security 182
4.7.9.4 Network Operations.....183
4.7.9.5 Network Processes.....184
4.7.9.6 Network Lab 184
4.7.9.7 Hardware Description 184
4.7.9.8 Hardware Refresh 185
4.7.10 Collaboration Services 185
4.7.10.1 JSC Video Teleconference Rooms 185
4.7.11 Customer Relationship Management 185
4.7.12 IT Security.....191
4.7.13 Cable Plant Services.....191
4.7.13.1 Optical Fiber 192
4.7.13.2 Twisted Pair Copper Cabling.....192
4.7.14 Emergency Warning Systems (RESERVED).....192
4.7.15 Public Address Systems (RESERVED).....192
4.7.16 Radio Services (RESERVED) 192
4.7.17 Telephone Services 192
4.7.17.1 System Overview.....192
4.7.17.2 Handsets.....193
4.7.17.3 Voicemail Services 194

4.7.17.4 E-911 Services 194
4.7.17.5 Trunks 194
4.7.18 Voice over Internet Protocol (VoIP) 194
4.7.19 Cable Television Services (RESERVED) 195
4.7.20 Continuation of Center Zoned Architecture Project (CZAP) 195
4.7.21 Ongoing Center-Specific Projects 195
4.7.22 Work Load Indicators 196
4.7.22.1 JSC Workload Indicators 196
4.7.22.2 WSTF Workload Indicators 197
4.7.23 Applicable Documents 197
4.8 KENNEDY SPACE CENTER (KSC) 198
4.8.1 Property/Inventory 198
4.8.2 Shipping/Receiving/Inspection Services 199
4.8.3 Vehicle Management 199
4.8.4 Physical Security 200
4.8.5 Emergency Management 200
4.8.5.1 Center Specific COOP Support 201
4.8.5.2 Service Continuity of Operations Support 201
4.8.6 Safety 201
4.8.7 Facilities 204
4.8.8 Network Services 205
4.8.8.1 IPAM 205
4.8.8.2 Remote Access Services 205
4.8.8.3 Network Time Protocol (NTP) 206
4.8.8.4 Guest Network 207
4.8.9 Data Services 207
4.8.9.1 High Level LAN Description 207
4.8.9.2 Wireless Networks 209
4.8.9.3 Network Security 210
4.8.9.4 Network Operations 212
4.8.9.5 Network Processes 212
4.8.9.6 Network Lab 213
4.8.9.7 Hardware Description 214
4.8.9.8 Hardware Refresh 214
4.8.10 Collaboration Services 214
4.8.11 Customer Relationship Management 214
4.8.12 IT Security 217
4.8.13 Cable Plant Services (RESERVED) 219
4.8.14 Emergency Warning System (RESERVED) 219
4.8.15 Public Address Systems (RESERVED) 219
4.8.16 Radio Systems (RESERVED) 219

4.8.17 Telephone Services (RESERVED) 219
4.8.18 VoIP (RESERVED) 220
4.8.19 Cable Television Systems (RESERVED) 220
4.8.20 Continuation of Center Zoned Architecture Project (CZAP) 220
4.8.21 Ongoing Center-Specific Projects 220
4.8.22 Work Load Indicators 220
4.8.23 Applicable Documents 221
4.9 LANGELY RESEARCH CENTER (LaRC) 222
4.9.1 Property/Inventory 222
4.9.2 Shipping/Receiving/Inspection 222
4.9.3 Vehicles Necessary To Support Center Work 222
4.9.4 Physical Security 222
4.9.5 Emergency Management 222
4.9.5.1 Center Specific COOP Support 223
4.9.5.2 Service Continuity of Operations Support 223
4.9.6 Safety 223
4.9.7 Facilities 223
4.9.8 Network Services 225
4.9.8.1 IPAM 225
4.9.8.2 RAS 225
4.9.8.3 NTP 225
4.9.8.4 Guest Network 225
4.9.9 Data Services 226
4.9.9.1 High Level LAN Description 226
4.9.9.2 Wireless Networks 228
4.9.9.3 Network Security 228
4.9.9.4 Network Operations 229
4.9.9.5 Network Processes 230
4.9.9.6 Network Lab 230
4.9.9.7 Hardware Description 230
4.9.9.8 Hardware Refresh 234
4.9.10 Collaboration Services 234
4.9.11 Customer Relationship Management 234
4.9.12 IT Security 234
4.9.13 Cable Plant Service 234
4.9.13.1 Optical Fiber 234
4.9.13.2 Twisted Pair Copper Cabling 235
4.9.14 Emergency Warning Systems (RESERVED) 235
4.9.15 Public Address Systems (RESERVED) 235
4.9.16 Radio Services (RESERVED) 235
4.9.17 Telephone Services 235

4.9.17.1 System Overview 235
4.9.17.2 Replacement Phone System 235
4.9.17.3 Handsets 236
4.9.17.4 Voice Mail Services 237
4.9.17.5 E911 Services 237
4.9.17.6 Trunks 237
4.9.18 Voice over Internet Protocol (VoIP) 237
4.9.19 Cable Television Services 237
4.9.20 Continuation of Center Zoned Architecture Project (CZAP) 238
4.9.21 Ongoing Center-Specific Projects 239
4.9.21.1 LaRC New Town Concept Project 239
4.9.22 Work Load Indicators 239
4.9.23 Applicable Documents 240
4.10 MARSHALL SPACE FLIGHT CENTER (MSFC) 241
4.10.1 Property/Inventory 242
4.10.2 Shipping/Receiving/Inspection 242
4.10.3 Vehicles Necessary to Support Center Work 242
4.10.4 Physical Security 242
4.10.5 Emergency Management 242
4.10.5.1 Center Specific COOP Support 242
4.10.5.2 Service Continuity of Operations Support 243
4.10.6 Safety 243
4.10.7 Facilities 243
4.10.8 Network Services 245
4.10.8.1 IPAM 245
4.10.8.2 RAS 245
4.10.8.3 NTP 245
4.10.8.4 Guest Network 245
4.10.9 Data Services 245
4.10.9.1 MSFC LAN High Level Description 245
4.10.9.2 MAF LAN High Level Description 246
4.10.9.3 NSSTC LAN High Level Description 247
4.10.9.4 Wireless Networks 248
4.10.9.5 Network Security 249
4.10.9.6 MSFC LAN Network Operations 249
4.10.9.7 MAF LAN Operations 250
4.10.9.8 NSSTC LAN Operations 251
4.10.9.9 Network Processes 251
4.10.9.10 Network Lab 251
4.10.9.11 Hardware Description 252
4.10.9.12 Hardware Refresh 254

4.10.10 Collaboration Services 254
4.10.11 Customer Relationship Management 254
4.10.12 IT Security....255
4.10.12.1 MSFC IT Security....255
4.10.12.2 NSSTC and MAF IT Security....255
4.10.13 Cable Plant Services (RESERVED) 255
4.10.14 Emergency Warning Systems (RESERVED)....256
4.10.15 Public Address Systems (RESERVED)....256
4.10.16 Radio Services (RESERVED) 256
4.10.17 Telephone Services (RESERVED)....256
4.10.18 Voice over Internet Protocol (VoIP) (RESERVED)....256
4.10.19 Cable Television Services (RESERVED)....256
4.10.20 Continuation of Center Zoned Architecture Project (CZAP) 256
4.10.21 Ongoing Center-Specific Projects....256
4.10.22 Work Load Indicators 256
4.10.23 Applicable Documents....257
4.11 NASA SHARED SERVICES CENTER (NSSC) 258
4.11.1 Property/Inventory 258
4.11.2 Shipping/Receiving/Inspection 258
4.11.3 Vehicles Necessary to Support Center Work....258
4.11.4 Physical Security....258
4.11.5 Emergency Management....258
4.11.6 Safety 258
4.11.7 Facilities 259
4.11.8 Network Services 259
4.11.8.1 IPAM....259
4.11.8.2 RAS....259
4.11.8.3 NTP 259
4.11.8.4 Guest Network 259
4.11.9 Data Services....259
4.11.9.1 High Level LAN Description....260
4.11.9.2 Wireless Networks....260
4.11.9.3 Network Operations....260
4.11.9.4 Network Processes....261
4.11.9.5 Network Lab 261
4.11.9.6 Hardware Description 261
4.11.9.7 Hardware Refresh 262
4.11.10 Collaboration Services 262
4.11.11 IT Security....262
4.11.12 Customer Relationship Management (CRM)....263
4.11.13 Cable Plant Services....263

4.11.14 Emergency Warning Systems 263
4.11.15 Public Address Systems (RESERVED) 263
4.11.16 Radio Services (RESERVED) 263
4.11.17 Telephone Services 264
4.11.18 Voice over Internet Protocol (VoIP) 264
4.11.19 Cable Television Services 264
4.11.20 Continuation of Center Zoned Architecture Project (CZAP) 265
4.11.21 Ongoing Center-Specific Projects 265
4.11.22 Work Load Indicators 265
4.11.23 Applicable Documents 265
4.12 STENNIS SPACE CENTER (SSC) 266
4.12.1 Property/Inventory 266
4.12.2 Shipping/Receiving/Inspection 266
4.12.3 Vehicles Necessary To Support Center Work 266
4.12.4 Physical Security 266
4.12.5 Emergency Management 267
4.12.5.1 Center Specific COOP Support 267
4.12.5.2 Service Continuity of Operations Support 267
4.12.6 Safety 267
4.12.7 Facilities 267
4.12.8 Network Services 268
4.12.8.1 IPAM 268
4.12.8.2 Remote Access 268
4.12.8.3 NTP 268
4.12.8.4 Guest Network Services 268
4.12.9 Data Services 269
4.12.9.1 High Level LAN Description 269
4.12.9.2 Wireless Networks 270
4.12.9.3 Network Security 271
4.12.9.4 Network Operations 271
4.12.9.5 Network Processes 273
4.12.9.6 Network Lab 273
4.12.9.7 Hardware Description 273
4.12.9.8 Hardware Refresh 274
4.12.10 Collaboration Services 274
4.12.11 Customer Relationship Management 274
4.12.12 IT Security 275
4.12.13 Cable Plant Services (RESERVED) 275
4.12.14 Emergency Warning Systems (RESERVED) 275
4.12.15 Public Address Systems (RESERVED) 275
4.12.16 Radio Services (RESERVED) 275

4.12.17 Telephone Services (RESERVED) 275
4.12.18 Voice over Internet Protocol (VoIP) (RESERVED) 275
4.12.19 Cable Television Services (RESERVED) 275
4.12.20 Continuation of Center Zoned Architecture Project (CZAP) 275
4.12.21 Ongoing Center-Specific Projects 276
4.12.22 Work Load Indicators 276
4.12.23 Applicable Documents 276

5 INFRASTRUCTURE PROJECTS 277
5.1 UNITES NISN NETWORK COMMUNICATIONS INTIATIVE (NCI) PROJECT 277
5.2 CENTER ZONED ARCHITECTURE PROJECT (CZAP) 278
5.3 FUTURE MULTI-CAST OPEN SHORT PATH FIRST (MOSPF) PROJECT 278
5.4 FUTURE OCIO/I^{3}P INFRASTRUCTURE PROJECTS 279
5.5 APPLICABLE DOCUMENTS 279

6 UNIQUE SERVICES 280
6.1 UNITeS RUSSIA IT SERVICES 280
6.1.1 UNITeS Russia IT Services Overview 281
6.1.2 Russia IT WAN and LAN and End User Support 282
6.1.2.1 Russia Hub/Synterra; Moscow 282
6.1.2.2 NASA Moscow Liaison Office (NMLO) ; United States Embassy 282
6.1.2.3 Volga Apartments; Moscow 283
6.1.2.4 Gagarin Cosmonaut Training Center (GCTC); Star City 283
6.1.2.5 Rocket Space Corporation-Energia (RSC-E) 283
6.1.2.6 Khrunichev State Research and Production Space Center283
6.1.2.7 Russian Space Agency (RSA) 284
6.1.2.8 Mission Control Center-Moscow (MCC-M) 284
6.1.2.9 Institute of Bio-Medical Problems (IBMP) 284
6.1.2.10 Baikonur or Kazak Cosmodrome; Kazakhstan 285
6.1.2.11 JSC Buildings 30 and 17 285
6.1.2.12 MSFC Building 4200 285
6.1.2.13 Russia IT Infrastructure 286
6.1.3 UNITeS Russia IT Security 291
6.1.4 Russia IT Technology Shipping, Export Control and Equipment Inventory 291
6.1.4.1 Russia IT Unique Export Control 291
6.1.4.2 Russia IT Subcontracting 292
6.1.4.3 Russia Unique VISA 293

6.1.4.4 Russia Unique Procurement....294
6.1.4.5 Russia Unique Insurance....294
6.1.5 Work Load Indicators....294
6.1.5.1 Direct Labor Hours....294
6.1.6 Operating Procedures....294
6.1.7 Applicable Documents....295
6.2 UNITeS NATIONAL SECURITY SYSTEMS (NSS) SERVICE IT SUPPORT296
6.2.1 UNITeS NSS Service IT Support Locations....296
6.2.2 UNITeS NSS IT Support Work Load Indicators....297
6.3 UNITeS DIGITAL TELEVISION (DTV) ENGINEERING SERVICE....297
6.3.1 Major Activities....298
6.3.2 Work Load Indicators....299
6.3.3 Applicable Documents....299

1 NICS BACKGROUND AND HISTORICAL

1.1 DISCLAIMER

The background and historical data contained herein is not intended to restrict prospective offerors in their approach to proposal preparation. This information is provided for the sole purpose of giving all offerors a better understanding of the requirements contained in this solicitation. The information provided constitutes a snapshot within a certain period of time, Fiscal Years 2007 (FY07), 2008 (FY08) and a portion of 2009 (FY09). The historical data provided herein is subject to modifications due to hardware/software technology changes, changing information resource management philosophies, current trends and new developments, and other factors. This historical data does not necessarily reflect the optimum approach for performing the work requirements and, further, should not be construed as being precise parameters governing the size of the effort. Further, the quantity of work to be performed may vary as the Center workload expands, or changes, due to changing roles of NASA Centers and NASA. Such changes are considered to be within the general scope of the NICS contract.

1.2 NASA IT OVERVIEW

NASA is comprised of NASA Headquarters (HQ) located in Washington, D.C., ten (10) Centers located throughout the continental United States, and a number of additional installations that support specific Centers (e.g. Center Associated Facilities). NASA HQ's role, the five strategic Enterprises' roles, and the Centers' roles are each distinct in carrying out the NASA mission. In consonance with the nation's leadership and priorities, HQ defines the NASA mission that the various Enterprises are subsequently charged with executing and implementing. The Centers are responsible for the alignment of the resources to implemented, and execute Agency-wide programs.

NASA conducts its work under the following four mission directorates:

a. Aeronautics: pioneers and proves new flight technologies that improve our ability to explore and which have practical applications on Earth.
b. Exploration Systems: creates new capabilities and spacecraft for affordable, sustainable human and robotic exploration.
c. Science: explores the Earth, Moon, Mars and beyond; charts the best route of discovery; and reaps the benefits of Earth and space exploration for society.
d. Space Operations: provides critical enabling technologies for much of the rest of NASA through the space shuttle, the International Space Station and flight support.

1.3 IT INFRASTRUCTURE IMPROVEMENT PROGRAM (I^3P)

The purpose of Information Technology (IT) at NASA is to enable the mission and deliver mission value through the use of IT services. To achieve this purpose, the OCIO defined the following vision, *NASA OCIO Strategy for Improving IT Management at NASA*, for the future of IT at NASA, based on the following strategies:

a. NASA invests in the right IT solutions that provide the greatest benefit to the NASA mission.
b. IT systems are seamlessly deployed and utilized across Center boundaries.
c. IT projects selected and executed by NASA provide expected benefits, such as return on investment, improved collaboration capability, improved security, etc.
d. IT at NASA makes information accessible, integrated and actionable for mission programs.
e. NASA CIO's provide a reliable, efficient, secure, and well-managed IT infrastructure that customers rely on rather than compete with.
f. NASA CIO's are credible, trusted partners in solving mission and business problems.

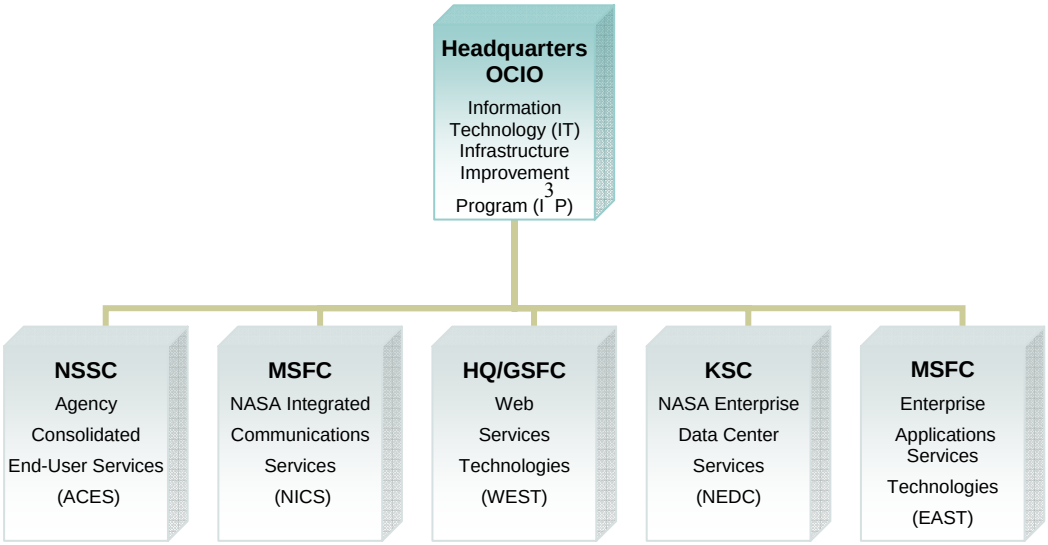
In order to effectively support the new vision for space exploration, the IT infrastructure of NASA must therefore undergo a significant transformation. To accomplish this, the NASA HQ's Office of the Chief Information Officer (OCIO) has initiated the Information Technology (IT) Infrastructure Improvement Program (I^3P), http://i3p-acq.ksc.nasa.gov. The key principles guiding I^3P are:

a. MISSION ENABLING: Information technology at NASA serves to enable NASA's mission.
b. INTEGRATED: NASA will implement information technology that enables the integration of business (mission) processes and information across organizational boundaries.
c. EFFICIENT: NASA will implement information technology to achieve efficiencies and ensure that IT is efficiently implemented.
d. SECURE: NASA will implement and sustain secure information technology solutions.

The expected benefits of I^3P are:

a. Seamless IT infrastructure that enables collaboration
b. Significant reduction in operating costs
c. Reduced complexity for managing IT services across the Agency
d. Improved IT security

As part of the I^3P strategy, it was decided to assign responsibility for implementation of the five I^3P acquisitions as follows:



In implementing the NASA HQ CIO's vision for I^3P, the decision was made to utilize the ITIL V3 framework to govern performance of the I^3P effort and to establish a common terminology across all of the I^3P contracts. ITIL is a commonly accepted information technology service management framework that provides a cohesive set of public and private sector best practices which are supported by a comprehensive qualifications scheme, accredited training and certification organizations, and implementation and assessment tools.

1.3.1 Enterprise Service Desk (ESD) (Tier 1)

The consolidated enterprise wide Tier 1 Service Desk (ESD), that all I^3P contractors will use, will be provided by NASA Shared Services Center (NSSC). The description of this service can be found on the I^3P website http://i3p-acq.ksc.nasa.gov/

1.3.2 Enterprise Service Request System (ESRS)

The consolidated enterprise wide IT Enterprise Service Request System (ESRS), that all I^3P contractors will use, will be provided by NASA Shared Services Center (NSSC). The description of this service can be found on the I^3P website http://i3p-acq.ksc.nasa.gov/

1.3.3 NASA Enterprise Data Center (NEDC)

NEDC will provide enterprise data centers services for NASA. The description of NEDC services can be found on the I^3P website:
http://i3p-acq.ksc.nasa.gov/Contracts/ Contract13.cfm

1.3.4 Agency Consolidated End-User Services (ACES)

ACES will provide end user device services for NASA. The description of ACES services can be found on the I^3P website:
http://prod.nais.nasa.gov/cgi-bin/eps/synopsis.cgi?acqid=133418

1.3.5 Enterprise Application Service Technology (EAST)

EAST will provide enterprise wide application services for NASA. The description of EAST services can be found on the following I^3P websites:
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=2
http://prod.nais.nasa.gov/cgi-bin/eps/synopsis.cgi?acqid=133176

1.3.6 Web Enterprise Service Technology (WEST)

WEST will provide enterprise wide web services for NASA. The description of WEST services can be found on the I^3P website:
http://i3p-acq.ksc.nasa.gov/Contracts/Contract14.cfm

1.4 NICS COORDINATION WITH CENTER INFORMATION OFFICES (CIO)

1.4.1 Coordination with MSFC IT Services (MITS)

The NICS civil servants and contractor will ultimately be accountable to the Agency CIO I^3P organization for service strategy, design, and operations, as stated in Attachment J-1, Appendix A, Section 2, *IT Service Management: Organization and Governance within NASA*. The MSFC CIO shares operational responsibility for NICS performance with the OCIO because the contract is hosted by MSFC, As such, the NICS civil servants and contractor will be expected to coordinate with the MSFC CIO's MITS contractor to flow contract status, risks, issues, IT Security and other information to the MSFC CIO, who will ultimately provide this information to the MSFC Center Director. The NICS civil servants and contractor will also be required to ensure that the necessary IT governance, Enterprise Architecture, IT Security, Financial Reporting, and Project Management requirements are consistent with MSFC policies and procedures, working with the MITS contractor in their MSFC IT support role. The MITS contract, currently scheduled for award in late 2009 by the George C. Marshall Space Flight Center (MSFC), provides IT services for the MSFC under the authority of the MSFC CIO. The MSFC OCIO is responsible for all MSFC IT related functions, including the development of Center IT strategies, IT architecture, IT investment management and tracking, and IT customer relationship management.

Documentation that explains the MSFC IT governance model is as follows:

a. *MSFC Center IT Governance and Organization Alignment Plan*
b. *MSFC Strategy and Investment (IT SIB) Board Charter*
c. *MSFC Enterprise Architecture Advisory Committee (MEAAC)*

The description of MITS can be found on the MSFC websites:
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=3
http://mits.msfc.nasa.gov/

1.4.2 Coordination with Center CIOs

The NICS services are an essential part of the Center CIOs' responsibility to the Center Director(s). The NICS civil servants and contractors will engage in extensive coordination, collaboration and communications with the Center CIOs' staff to meet Center expectations and achieve customer satisfaction.

1.5 NICS OVERVIEW

The NICS contract will include the following key areas:

a. Contract Management: These services include program management, financial management, logistics, contract Phase-In/Transition management, procurement, security management, safety, health & environmental management, facilities management, quality assurance and management, contractor's role in I^3P, other interface points, and contract and subcontract administration.

b. Enterprise Services: These services include network services, voice services, data services, collaboration services, corporate management and operations, mission services, mission management and operations, customer relationship management, service management, strategy generation, IT security support, and GSA contract integration. This is to include WAN and LAN communication services at all NASA Centers and associated component facilities.

c. Center and Associated Component Facility Services: These services include Center and associated component facility-specific services, such as cable plant management, Emergency Warning System (EWS), public address system, radio, telephone service, Voice over Internet Protocol (VoIP), cable television (TV).

d. Infrastructure Projects: This activity includes both continuation and new projects and shall include all the effort to perform projects such as Network Communications Initiative (NCI) Continuation Project, Center Zone Architecture Program (CZAP) Continuation Project, NICS Consolidated Configuration Management System, Consolidated Corporate Network Operations Center Project, and other NASA-approved projects. These projects shall be accomplished in accordance with NPR 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*.

e. Unique Services: These services include infrastructure (i.e. desktop, LAN management) for Russia IT services, NASA National Security Systems (NSS) service IT support, and Digital Television (DTV) engineering services.

1.5.1 Existing NASA Contracts that Become Part of NICS

The NICS initiative will require the consolidation of portions of numerous contracts across the Agency that currently include the services defined in NICS. These existing contracts include:

a. The NASA Integrated Services Network (NISN) effort currently provided by the "Unified NASA Information Technology Services (UNITeS)" contract NNM04AA02C.
b. The local area network efforts currently provided under a number of Center "Outsourcing Desktop Initiative for NASA (ODIN)" Delivery Orders.
c. The local area network efforts not covered by ODIN that are included in Center specific contracts.
d. The NICS contractor will be responsible for the Phase-In of activities for contracts that become part of NICS at contract assumption.
e. Additionally, the contractor will be responsible for the transition activities for contracts that become part of NICS after contract Phase-In. These additional contract moves to NICS are referred to as Transition.

The expected contracts and the associated Phase-In or Transition dates are provided in the RFP as Attachment J-19, *Contract Phase-In and Transition Schedule*.

Phase-In activities include such activities as:

a. Hiring of incumbent personnel, if proposed, that will become part of the NICS employee prime or subcontractor team.

b. Coordination with each Center Safety, Health, & Environmental (S&MA) representatives to facilitate the preparation and submission of a comprehensive Center-specific Safety and Health Plan.

c. Transition of existing Government property, if requested, from current contracts to the NICS contract as defined in NICS RFP Attachments J-8, *Government Furnished Property*, and J-9, *Installation Accountable Government Property.*

d. Preparation and submission of comprehensive and complete subcontract packages to the Contracting Officer for consent to subcontract.

e. Coordination with the NASA technical monitors for the transition of services.

f. Coordination with NASA to establish the interface between the Contractor's financial management system and NASA's financial and cost reporting requirements.

g. Other activities necessary to assume full contractual responsibility of all NICS contract functions by the required date.

The contractor's Transition activities will include all activities as delineated above for the additional contracts that are transitioned into NICS subsequent to full contract assumption. The key difference is that the contractor will be providing the previously consolidated services of contracts that transferred during the Phase-In period.

Copies of the contracts as delineated in the RFP at Attachment J-19, *Contract Phase-In and Transition Schedule* may be requested in writing from that Center's Freedom of Information Act Offices as follows:

a. NASA Ames Research Center, Attn: FOIA Public Liaison Officer , MS 943-4, Moffett Field, CA 94035-1000
Phone: (650)604-3273, foia@arc.nasa.gov
b. NASA Dryden Flight Research Center, Attn: FOIA Public Liaison Officer 4800 Lilly Drive Bldg. 4839, Edwards, CA
Phone: (661)276-3449, Fax: (661)276-3566
foia@dfrc.nasa.gov
c. Glenn Research Center, Attn: GRC FOIA Public Liaison Officer , Mail code: 500-313, Cleveland, OH 44135
Phone: (216)433-2813
foia@grc.nasa.gov
d. NASA Headquarters, Attn: FOIA Public Liaison Officer, 300 E Street, SW Room 9R35, Washington, DC 20546
Phone: (202)358-2265 & (202)358-0845, Fax: (202)358-4331 foia@hq.nasa.gov
e. NASA Goddard Space Flight Center, Attn: Freedom of Information Office Code 130,Greenbelt, Maryland 20771
Fax: (301)286-1712
foia@gsfc.nasa.gov
f. Johnson Space Center, Attn: FOIA Public Liaison Officer , Johnson Space Center Mail code: AP2, Houston, Texas 77058
Phone: (281)483-8612
foia@jsc.nasa.gov
g. John F. Kennedy Space Center, Attn: XA-A1/FOIA Customer Service Center, Kennedy Space Center, FL 32899
Phone: (321)867-9280, Fax: (321)867-8007
foia@ksc.nasa.gov
h. NASA Langley Research Center, Attn: Freedom of Information Act Office, 17 Langley Blvd. Mail Stop 412, Hampton, VA 23681
Phone: (757)864-2497, Fax: (757)864-6477
LARC-DL-foia@mail.nasa.gov
i. NASA, George C. Marshall Space Flight Center, Attn: Freedom of Information Act Office, CS20, MSFC, AL 35812
foia@msfc.nasa.gov

j. Stennis Space Center, Attn: Freedom of Information Act, Office, 1100 , Stennis Space Center, MS 39529
Fax: 1-866-779-NSSC, ssc-foia@nasa.gov ,
http://www.nasa.gov/centers/stennis/about/foia/index.html

k. NASA Shared Services Center (NSSC), Attn: Freedom of Information Act, Office, 1111, C Road , Stennis Space Center, MS 39529
Fax: 1-866-779-NSSC, nssc@nasa.gov,

1.5.2 Tours of Duty

Normal Center duty hours are provided for the offeror's information. Normal Center duty hours are typically defined as:

a. Five (5) day week, Monday through Friday (excluding holidays)
b. Eight (8) hours per day between 6:00 a.m. and 6:00 p.m.

Offerors will be expected to establish working hours compatible with the Center organizations to be supported. Sections 3, 4, and 6 define operational support that is required, if any, outside of normal duty hours.

1.5.3 NICS Location of Performance:

NICS contract effort will occur at NASA Headquarters and the ten (10) Centers, Centers' Associated Component Facilities (as defined in Section 4.0), Jet Propulsion Lab (JPL, note WAN only), and Russia.. The PWS delineates the official places of performance for the NICS contract. In order to provide the greatest amount of relevant information regarding the Centers at which effort will occur, the following links are provided. These sites provide information relating to each Center's mission, their organizational structure, and points of contact.

a. Ames Research Center (ARC)
http://www.nasa.gov/centers/ames/home/
b. Dryden Flight Research Center (DFRC)
http://www.nasa.gov/centers/dryden/about/index.html
c. Glenn Research Center (GRC)
http://www.nasa.gov/centers/glenn/home/
d. Goddard Space Flight Center (GSFC)
http://www.nasa.gov/centers/goddard/home/
e. GSFC's Wallops Flight Facility (WFF)
http://www.nasa.gov/centers/wallops/home/index.html
f. NASA Headquarters (HQ)
http://www.nasa.gov/centers/hq/home/
g. HQ's NASA Management Office-JPL
http://www.nasa.gov/centers/jpl/home/index.html
h. Johnson Space Center (JSC)

http://www.nasa.gov/centers/johnson/home/

i. JSC's White Sands Test Facility
http://www.nasa.gov/centers/wstf/home/

j. JSC's El Paso Hanger
http://www.nasa.gov/centers/johnson/home/

k. John F. Kennedy Space Center (KSC)
http://www.nasa.gov/centers/kennedy/home/

l. KSC's Vandenberg AFB
http://www.nasa.gov/centers/kennedy/home/

m. KSC's Merritt Island Launch Annex
http://science.ksc.nasa.gov/facilities/mila.html

n. Langley Research Center (LaRC)
http://www.nasa.gov/centers/langley/home/index.html

o. George C. Marshall Space Flight Center (MSFC)
http://www.nasa.gov/centers/marshall/home/

p. MSFC's Michoud Assembly Facility (MAF)
http://www.nasa.gov/centers/marshall/michoud/index.html

q. MSFC's National Space Science & Technology Center (NSSTC)
http://www.nsstc.org/

r. MSFC's UNITeS NISN and Russia IT Services
http://www.nisn.nasa.gov

s. Stennis Space Center (SSC)
http://www.nasa.gov/centers/stennis/home/

t. NASA Shared Services Center (NSSC)
http://www.nssc.nasa.gov

1.6 DOCUMENT OVERVIEW

NICS will consolidate into one contract NASA's wide area networks (WANs) and local area networks (LANs) into an enterprise wide NASA Integrated Services Network (NISN). This consolidation includes all the services of existing NISN, currently provided by the UNITeS contract, as well as the GSFC Mission Operations Management Service (MOMS) Task Order 16 Mission services and all corporate Center LANs provided by ODIN and other center specific contracts. Refer to the RFP at Attachment J-19, *Contract Phase-In and Transition Schedule* for a list of all contracts that consolidate into NICS.

Additionally, this contract will provide for Center and Associated Component Facility Services (NICS PWS 4.0) and Unique Services (NICS PWS 6.0) that will not be part of NISN.

Finally, NICS will include key infrastructure improvement projects (PWS 5.0) that have been approved by NASA IT governance boards. These projects are considered complete once their objectives have been met and have transitioned into operations. These projects provide for the design, modernizations, or enhancements to the Enterprise services, infrastructure, tools and processes.

The NICS background and historical document is divided into six sections that loosely align with the NICS PWS:

a. Section 1 is an introductory discussion of the OCIO I^3P vision and collaboration with NICS.
b. Section 2 describes UNITeS contract management as a legacy reference for how similar efforts have been implemented.
c. Section 3 describes UNITeS and MOMS Task Order 16 NISN current services
d. Section 4 describes a variety of information to include:
   1) How IT services are performed at each Center.
   2) Current Center services that will be consolidating into the NICS definition of NISN (e.g. Enterprise Services), specifically LANs.
   3) Center and Associate Component Facility Services that, although are part of NICS, they are not part of NISN. This description includes existing contracts that will be consolidated into NICS.
e. Section 5 current projects that will be continued in NICS and a brief description of future possible Indefinite Delivery/Indefinite Quantity (IDIQ) projects.
f. Section 6 describes those Unique Services that are currently part of UNITeS that will consolidate into NICS to include:
   1) UNITeS Russia IT Services
   2) UNITeS NASA National Security Systems (NSS) IT Services
   3) UNITeS DTV Engineering Services

Each document section includes an applicable documents list. Each list identifies the document and the location of the document. Document locations range from NASA public websites (e.g. http://i3p-acq.ksc.nasa.gov) to the MSFC Acquisition Portal Reading Room (e.g. http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1).

1.7 APPLICABLE DOCUMENTS

The following is a listing of applicable documents for background and historical section 1.0.

Located at the I^3P Technical Library http://i3p-acq.ksc.nasa.gov

a. NASA OCIO Strategy for Improving IT Management at NASA

Located at the MSFC FOIA Office http://foia.msfc.nasa.gov/ (See section 1.5.1)

a. *Unified NASA Information Technology Services (UNITeS),* Contract Number, NNM04AA02C
b. UNITeS Contract, Attachment J-1, *UNITeS Performance Work Statement (PWS)*
c. UNITeS Contract, Attachment J-2, *Data Procurement Document*

d. UNITeS Contract, Attachment J-3, *Wage Determination*s
e. UNITeS Contract, Attachment J-4, *Performance Measurement Standards*

Located at the Executive Orders:
(http://www.archives.gov/federal-register/executive-orders/)

a. Executive Order 013495, *Non-Displacement of Qualified Workers under Service Contracts*

Located at the NICS, Other Documents, B&H Applicable Documents
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. *MSFC Center IT Governance and Organization Alignment Plan,* (MSFC IT Governance and OA Plan IMSB-Plan-2800 1.pdf)
b. *MSFC Enterprise Architecture Advisory Committee (MEAAC) Charter,* (MSFC MEAAC Charter_Signed.pdf)
c. *MSFC Strategy and Investment (IT SIB) Board Charter,* (IT SIB MSFC Charter MC-30.pdf)

2 UNITeS CONTRACT MANAGEMENT

The following background and historical information is only related to what is currently provided to NASA by the UNITeS contractor. This information is provided because it is a legacy reference for how efforts of similar complexity are currently provided by UNITeS.

The UNITeS contract, in redacted form, is available from the MSFC Freedom of Information Act Office, and may be requested in writing. In lieu of delineating within this document a comprehensive description of all services provided under the UNITeS contract, interested parties may review the UNITeS Contract Attachment J-1, *UNITeS Performance Work Statement (PWS)*. For instance, UNITeS Contract, Attachment J-2, *Data Procurement Document*, will provide a detailed description of all UNITeS reporting and documentation requirements. UNITeS contract, Attachment J-4, *Performance Standards*, delineates the objective performance metrics against which certain sections of contractor performance are measured.

The UNITeS contract, NNM04AA02C, supports both MSFC and Agency requirements. Science Applications International Corporation (SAIC) is the UNITeS prime contractor. The contract start date was January 1, 2004 (with a 90-day phase-in period) and was awarded for a period of performance of five years, including options. The UNITeS contract has since been fully extended to the end April 2010 and thus support the NICS contract start date of May 01, 2010.

The UNITeS contractor's mission is to manage, be responsible for, and provide IT services to meet the requirements defined by the UNITeS PWS. The UNITeS contractor provides the following:

a. Operates and maintains existing equipment, software and services
b. Gathers, analyzes, defines, and documents systems requirements
c. Plans, designs, develops or acquires, integrates, tests, and implements new systems or enhancements to existing systems.

The UNITeS services include the following:

a. Agency-wide Information Services (PWS 3.0): These services include IT Security, National Security Systems, wide area network (NISN), control center, data center, applications, Digital Television (DTV), Russia IT support, and customer services. These services also include development and maintenance of Agency-wide applications, services, and systems delegated to MSFC.

b. Integrated Enterprise Management Program (IEMP) Integration Services (PWS 4.0): These services are provided to the IEMP Integration Project Office (IPO) at MSFC and include infrastructure support, module project support, and operations and sustaining support.

c. Marshall Space Flight Center (MSFC) Information Services (PWS 5.0): These services include IT systems support for programs and projects for which MSFC is responsible. These services include applications software, web, midrange computer systems, telecommunications, IT security, audiovisual information, documentation repository, hardware maintenance, IT procurement, and customer support.

The UNITeS contract has provisions for procurement of necessary computer equipment, telecommunications equipment, software, and other IT related items and services required to support MSFC and the Agency. Accepting, tracking, and resolving problems and requests for assistance are an integral part of the contractor's responsibilities. All software in place is NASA-owned and is not proprietary to the UNITeS contractor.

Although UNITeS documentation will provide insight into current activities, the contract will not be re-competed in its present form. Portions of UNITeS will be competed as four separate and distinct acquisitions.

a. I^3P - NASA Integrated Communications Services (NICS) - Previously a portion of UNITeS Agency-wide Information Services, PWS 3.0
b. I^3P - Enterprise Applications Service Technologies (EAST) - Previously UNITeS Integrated Enterprise Management Program (IEMP) Integration Services, PWS 4.0
c. I^3P - NASA Enterprise Data Center Services (NEDC) - Previously a portion of UNITeS Agency-wide Information Services, PWS 3.0
d. MSFC Information Technology Services (MITS) - Previously MSFC Information Services, PWS 5.0

The breakout of UNITeS services into the following distinct acquisitions is provided in *UNITeS Mapping to New Procurements*.

2.1 UNITES PROGRAM MANAGEMENT

The contractor provides an integrated program management function with oversight and responsibility of both Agency and MSFC services. The contractor performs management activities necessary to plan, execute, control, and report project performance, timelines, events, risk and resource coordination. The UNITeS program management consists of Project Management, Financial Management, Contract Administration, Procurement Management, Asset Management, Security, Safety, Facilities Management, Quality Assurance, and Contract Documentation.

2.1.1 UNITeS Risk Management

The contractor maintains a continuous risk management program throughout the life of the contract. The contractors risk management program was effectively aligned with the processes established by the MSFC CIO *Organizational Work Instruction, Information Technology Risk Management (IS-01-008)* and with the Center and Agency directives for continuous risk management. The contractor utilizes the ePORT risk management tool to capture, track, and manage UNITeS program and project risks (note: NICS project risk are included in NICS PWS 5.0) on an ongoing basis. The contractor conducted monthly risk management reviews with program/project management staff and civil service monitors. For each risk identified, the contractor developed a statement of risk, assigned specific ownership to a risk owner, identified the likelihood and consequence, developed appropriate watch/mitigation strategies, and reviewed, tracked, and reported the status on an ongoing monthly basis.

2.2 UNITES FINANCIAL MANAGEMENT

Financial Management includes integrated management information systems, as well as planning and control systems to provide for the planning, tracking, accumulating, and reporting of contract (negotiated) cost versus actual costs to maximize resources utilization. This element also involves other financial support required to meet the budgeting, cost reporting, billing, and disclosure requirements of the contract.

2.2.1 UNITeS Management Information Control System (MICS)

Although NICS does not require the use of MICS, the following background and historical information is provided to help the contractors understand the purpose of the financial management (e.g. NICS DRD 1294MA-012, *Financial Management Report (533M & 533Q)* and cost reports (e.g. NICS DRD1294MA-010, *Cost Reports*). Additionally this should provide insight into what the contractor's provided financial management system will need to provide to meet the financial and cost reporting functionality of for NICS. NICS plans to use the concept of a "NICS NASA defined Work Package" as the basic structure to budget and track work performed on NICS (reference NICS DRD 1294MA-010, *Cost Reports*).

The UNITeS provides, implements, and maintains a NASA specific financial management information system, e.g. MICS. The system tracks the status of contractor's individual procurements from purchase request through final purchase order, delivery, and acceptance and provides appropriate information to the Integrated Enterprise Management (IEM) system. MICS is government-owned software that is built around an Oracle database with SQL forms. The MICS application is hosted on a Linux server. Currently the system, MICS 2.3.0 provides for the following:

a. Number of Users: 350 (including both NASA Users and UNITeS Users)
b. Software:
    1) Oracle Application Server 10g
    2) Oracle Relational Database 10g
    3) Oracle Internet Development Suite 10g (Development team)
    4) Internet Browser (Client)
        a. Apple Mac - Safari
        b. PC - Internet Explorer or Firefox

This MICS includes the procurement and tracking of all required supplies/materials, equipment, software, and services, not otherwise furnished by the Government, necessary to accomplish the contract mission. Examples include replacement parts/equipment, spare parts for hardware maintenance, vendor maintenance agreements, emergency parts, temporary labor services; IT related supplies, software subscription services, hardware engineering change/updates, and special general purpose software packages.

As part of the services referenced above, UNITeS provides for acquisitions both as part of its responsibilities in meeting the requirements of the statement of work and also in support of customers providing funding for additional IT purchases which are outside of its normal responsibilities. Both types are considered to be within the scope of the UNITeS contract effort. However, the NICS contractor will only be required to provide similar cost and procurement reports in support of contract activities and will not support NASA customers in the acquisition of items that are not required to perform the NICS mission.

The following documents provide a more in-depth understanding of MICS:

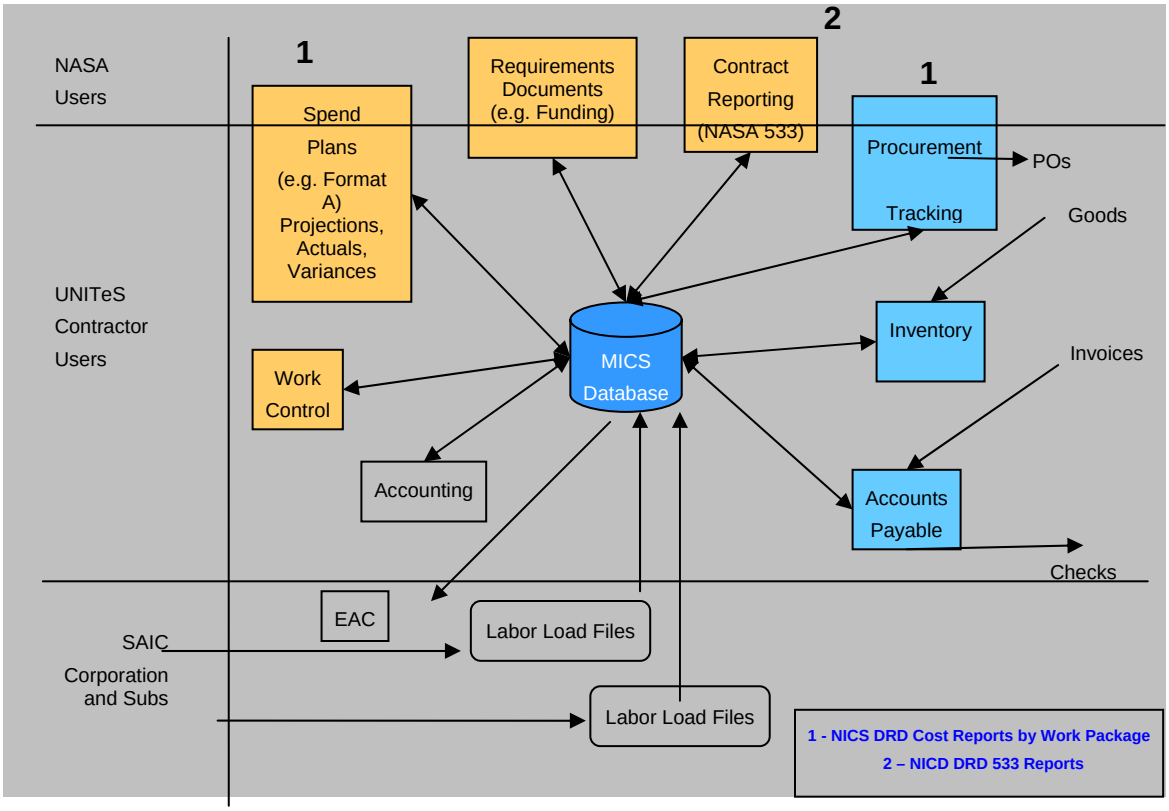
a. Management Information Control System (MICS) Accounts Payable User Operations Guide
b. Management Information Control System (MICS), User and Operations Guide (UOG) Purchase Requisition (PR) Funding Process
c. Management Information Control System (MICS), Project Control User Operations Guide
d. Management Information Control System (MICS), Purchase Requisition (PR) User and Operations Guide (UOG)
e. Management Information Control (MICS), Procurement Purchase Procedures

User Operations Guide

f. *Management Information Control System (MICS), Property User Operations Guide*
g. *Management Information Control System (MICS), User Operations Guide*

The emphasis in NICS is different from UNITeS in that NASA no longer intends to own the contract's financial management system (e.g. UNITeS MICS) but instead is expecting a contract-provided financial management system that will provide the electronic reports specified in DRD 1294MA-012, *Financial Management Report (533M & 533Q)* and DRD 1294MA-010, *Cost Reports*, that allows NASA technical monitor(s) the insight to review for budget planning, status reporting and procurement tracking (e.g. UNITeS term "spend plan"). This change will require the NICS contractor to configure the interfaces into and out of the contractor's financial management system so that NASA can receive reports in accordance the NICS DRDs listed above.

The document entitled *UNITeS MICS Sample Cost Reports* provides additional insight to how MICS interactive screen shots/outputs are used by NASA to track planned vs. actuals, projections and procurements. Additionally, since procurement tracking is a key part of DRD 1294MA-010, *Cost Reports*, the document entitled *NISN UNITeS Auto-Create MICS PRs*, provides insight in how NISN currently flows orders from engineering to purchase request creation. The figure below illustrates MICS today and indicates the division between NASA users and the UNITeS contractor users. The NICS DRDs are delineated by (1), DRD 1294MA-010, *Cost Reports*, and (2) DRD 1294MA-012, *Financial Management Report* (533M & 533Q).



2.2.2 UNITeS Integrated Enterprise Financial (IEF)

The UNITeS contractor supports the CIO resource analyst in evaluating the relevant UNITeS accounting information retrieved from the Integrated Enterprise Financial System (IEMP) (e.g. SAP). http://iemp.nasa.gov

2.2.3 UNITeS OMB Circular A-11, Exhibit 300

The UNITeS contractor annually assists the Government in completing contractual financial data relevant to NISN as required by OMB Circular A-11, Exhibit 300. The OMB Circular A-11, Exhibit 300 can be found at the following link:
http://www.whitehouse.gov/omb/circulars.

2.3 UNITES LOGISTICS

The UNITeS contractor performs property management and administration of all property acquired by, or in possession of, the contractor and subcontractors, including both Government-Furnished Property and Installation Provided Property and Equipment. RFP Attachments J-8, *Government-Furnished Property*, and J-9, *Installation Accountable Government Property,* delineate the list of equipment that will be consolidated into NICS and provided for contractor use.

2.3.1 UNITeS Property/Inventory Management

The UNITeS contractor conducts property inventories annually at each major NASA facility where UNITeS equipment is located.

2.3.2 UNITeS Shipping/Receiving/Inspection Services

The UNITeS contractor, in accordance with MSFC policies, provides for shipping, receiving and inspection services for all hardware/software procurements in support of the contract.

The current UNITeS receiving process is as follows:

a. The procuring onsite contractor has the vendor ship the items to the MSFC central receiving area, and provides MSFC Logistics Services Contractor with a copy of the purchase order (PO). When the shipment arrives, it is delivered to the procuring contractor's point of contact (per the packing slip and information provided on the PO previously).

b. The procuring contractor signs a DRAY ticket acknowledging receipt of the items. The procuring contractor has 5 days from receipt of the property to submit the form DD1149 to the Government.

c. The procuring contractor is required to provide on/with the DD1149 the information required per Federal Acquisition Regulation (FAR) Clause 52.245-1 (see NICS solicitation section I) to create the property record that contains such information as description, model number, manufacturer, serial number, acquisition cost, etc., either on the form or as an attachment. The Logistics Services Contractor logs the DD1149 and cross references the Purchase Order provided previously, tags the equipment, enters the property record, and assigns the property to the appropriate user (usually listed on the DD1149).

d. The procuring contractor keeps track of the property in accordance with their contract requirements.

More detailed shipping and receiving procedures can be found in the following applicable documents:

a. Reporting Movement of UNITeS Controlled Property Procedures, SOP 1B219
b. UNITeS Receipt of Property Procedure
c. Shipping UNITeS Property Procedure

Note: The above process is applicable only to the MSFC specific shipping and receiving process and does not reflect the complexity of NICS requirements. See Section 4.0 for additional information on Center specific shipping, receiving, and inspection services.

For NICS the contractor may access NASA Property, Plant and Equipment (PP&E) directly from either on site or off site location by using the NASA network services.

More detailed information on Property, Plant, and Equipment can be found in the following applicable documents:

a. *Federal Acquisition Regulation, Part 45, Government Property*
b. *NASA FAR Supplement, Part 1845, Government Property*
c. *NPD 4100.1, Supply Support and Material Management Policy*
d. *NPD 4200.1, Equipment Management*
e. *NPD 4300.1, NASA Personal Property Disposal Policy*
f. *NPR 4100.1, NASA Materials Inventory Management Manual*
g. *NPR 4200.1, NASA Equipment Management Procedural Requirements*
h. *NPR 4200.2, Equipment Management Manual for Property Custodians*
i. *NPR, 4300.1, NASA Property Disposal Procedural Requirements*
j. *NPR 9250.1, Property, Plant, and Equipment and Operating Materials and Supplies*
k. *N-PROP Quick Reference Guide*

2.3.3 UNITeS Vehicles

The UNITeS contractor provides leasing of motor vehicles from GSA in accordance with FAR 8.11 and NFS 1808.1100, *Leasing of Motor Vehicles*, NPD 6000.1, *Transportation Management*, and NPR 6200.1, *NASA Transportation and General Traffic Management*. In accordance with NFS 1851.202, *Contractor Use of Interagency Fleet Management System (IFMS) Vehicles,* the Center Transportation Officer must authorize all Interagency Fleet Management System (IFMS) vehicles assigned under cost reimbursable contracts. Also, NFS 1852.223-76, *, Federal Automotive Statistical Tool Reporting* , requires contractors to gain approval from their respective Center Contracting Officer (CO) and Transportation Officer (TO) prior to acquiring, replacing, and/or disposing of any NASA-owned or IFMS vehicles. Additionally, the contractor is required to transmit all requests to the Center TO, who will review and further process to GSA. The list of vehicles currently acquired by the contractor through GSA BOAC No. 804092 lease in support of UNITeS NISN is provided in *UNITeS NISN Vehicle List*. This list, which only applies to vehicles leased by UNITeS for NISN, includes all vehicles used at all NISN locations for both gateway and Customer Service Representatives (CSR) functions. The list is subject to change at time of award. The number of leased vehicles could possibly increase or decrease by a small number depending on justification for use.

Contractors who operate Government owned/leased vehicles must meet the requirements provided in the NASA compliance strategy as outlined in the applicable documents referenced in 2.3.3. This strategy describes the steps NASA will take in fulfilling the requirements of the Environmental Protection Act of 1992 and Executive Order 13149. *Greening the Government through Federal Fleet and Transportation Efficiency*. When practical, Alternative Fuel Vehicles

(AFV) will be used over non-AFVs during annual replacement plans, as well as, when new vehicle requests are received.

Vehicle requests must be initiated by the contractor using a NASA Form 1759, *Vehicle Justification*. Information included within this form must include designation of a contractor representative with whom the MSFC Motor Vehicle Fleet Operations Officer and/or Center representative. This individual will furnish information and assistance as required, including reasonable opportunities to observe motor vehicle operations and facilities and examine pertinent costs or other records. Such information may include inventory, management operation, storage of motor vehicles, vehicle use, mission needs, personnel involved, validation of applicable drivers license and applicable insurances, and how the need is currently being met. This process can be expedited by including as much of this information as possible with the original requesting documents. New requests should be received as far in advance as possible prior to issuing a request that proposed the use of GSA Fleet Vehicles (i.e., leased) in order to assess fleet availability. GSA typically orders new vehicles in the fall and winter for delivery in the following spring. It may be necessary to make short-term arrangements to fill any gap caused by vehicle acquisition lead-times. Coordinating early with COTR and starting the authorization process well in advance may avoid this potential problem. The only circumstance in which vehicle availability is generally not an issue is when the vehicles are already in place, either by assignment to NASA or to a preceding contractor. Even in such cases, however, all of the applicable requirements for authorization and approval for use must satisfy mission requirements. The contractor should not negotiate directly with GSA to acquire, dispose, or replace any Government owned/leased vehicle.

Contractors must also maintain a vehicle fleet database and provide the MSFC Transportation and Logistics Engineering Group and/or Center designated representative, updates when changes occur to fleet characteristics. Minimum entries to this database will include mileage, vehicle additions, replacements, deletions, vehicle cost data, vehicle descriptions, users, fuel type, and repair and maintenance information. Electronic submittals are preferred. Contractors who operate Government owned/leased vehicles are required to assemble and report Federal Automotive Statistical Tool (FAST) data annually, no later than October 15th of each calendar year. Contractors are responsible for the entry of data directly into FAST. The MSFC Transportation and Logistics Engineering Group can assist the contractor by providing guidance or interpretation of FAST as needed.

A MSFC-appointed Vehicle Review Team will annually validate vehicle types, quantities, current fleet size, planned fleet sizes, fleet utilization, and AFV goals of all Government-owned, contractor operated vehicles to ensure proper allocation and utilization of vehicles based on program requirements. Vehicles identified as not meeting the GSA Miles-Traveled Guidelines must be re-justified each fiscal year with COTR approval. The VRT team will assess information provided with the NASA Form 1759 to ensure mission objectives clearly justify continued use of vehicle.

Note: The above process is applicable only to the MSFC specific vehicles under UNITeS and does not reflect the complexity of NICS requirements. See Section 4.0 for additional information on Center specific vehicles.

2.4 UNITES PROCUREMENT

Although NICS does not require the use of MICS, the following background and historical information is provided to help potential offerors understand the NICS cost reports (e.g. NICS DRD 1294MA-010, *Cost Reports*) that the offeror's financial management system needs to provide for procurement tracking.

The UNITeS contractor provides, implements, and maintains a procurement information system as part of the UNITeS Management Information Control System (MICS). The system tracks the status of individual procurements from purchase request through final purchase order, delivery, and acceptance and provides appropriate information to the Integrated Enterprise Management (IEM) system.

This function includes the procurement and tracking of all required supplies/materials, equipment, software, and services, not otherwise furnished by the NASA, necessary to accomplish the contract mission. Examples include replacement parts/equipment, spare parts for hardware maintenance, vendor maintenance agreements, emergency parts, temporary labor services; IT related supplies, software subscription services, hardware engineering change/updates, and special general purpose software packages.

As part of the UNITeS services referenced above, the contractor (through subcontractor Arcata Associates) provides for acquisitions both as part of its responsibilities in meeting the requirements of the performance work statement and also in support of MSFC customers providing funding for additional IT purchases which are not required by the UNITeS contractor to perform UNITeS effort. Both types are considered to be within the scope of the UNITeS contract effort. The NICS contractor will NOT provide acquisition services to support MSFC customers but will only acquire items and services, such as those delineated above, that are required to perform the NICS services.

The following is a breakout of the approximate number of UNITeS purchase orders generated during the last two calendar years of UNITeS in support of NISN:

UNITeS PWS	Number of Purchase Orders	Approximate Value	Date	Comment
3.0	644	$19,000,000	2007	
3.0	619	$17,000,000	2008	
4.0	1	$1,000	2008	IEM DNS Support purchased under NISN RD 230

5.0	8	$123,000	2007	NISN RD 500 for 24x7 operations center
5.0	10	$94,000	2008	NISN RD 500 for 24x7 operations center

Under a subcontract to UNITeS, SAIC currently provides NASA with an IDIQ procurement vehicle that allows the contractor to purchase the key networking line items. This pre-negotiated IDIQ equipment items allows for equipment to be purchased and available for deployment into NISN in ten (10) working days. The document, *NISN Procurement Metrics 12-08*, provides additional insight into the NISN specific procurements both regular and IDIQ.

2.5 UNITES SECURITY MANAGEMENT

Security management includes the preparation and implementation of a comprehensive security management plan consistent with applicable Department of Defense (DoD), NASA, and MSFC policies and procedures. Also included in this element are IT resources protection, personnel security, facility access procedures, policies and protection, and the safeguarding of Privacy Act Information and property data and classified information.

2.5.1 UNITeS Physical Security

UNITeS complies with the NASA Office of Security for Program Protection (OSPP) policy rules and guidelines that cover all NASA Center's and Center associated facilities. The following link provides additional data on OSPP directives on physical security http://www.hq.nasa.gov/office/ospp

2.5.2 UNITeS Information Technology (IT) Security

The following functions will be provided by MITS for the MSFC OCIO. The NICS contractor will coordinate with MITS to provide relevant NICS IT security information. This will provide the MSFC OCIO with the necessary information to assess NICS compliance with IT Security.

Working with the MITS contractor, the NICS contractor is expected to support the MSFC CIO IT Security with the following NICS-specific data related to:

a. Center IT Security Program
b. Center Information Systems Change Board (ISCB)
c. IT Security Policy, Procedures And Guidance
d. IT Security Training And Awareness
e. IT Security Risk Management
f. Computer Forensics And Investigation Support

For specific MITS information, refer to the following site:
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=3
http://mits.msfc.nasa.gov/

2.5.3 UNITeS Export Control

NISN and Russian Services support many NASA requirements in international locations. As a result, shipment of telecommunications equipment occurs to non-US locations. The UNITeS contractor is responsible for shipment of the necessary equipment to install, maintain, and manage IT services at these locations, in accordance with MSFC and NASA Export Control and Shipping Procedures.

The contractor is also required to attend the Monthly Export Control Representative meeting and yearly certification training sessions provided by the MSFC Export Control Program. Additional training of personnel is encouraged. The contractor is responsible for ensuring that its employees are aware of the procedures for all areas of export control, including, but not limited to: placing information on the world wide web; placing information in the Public Domain (i.e. International conference, trade magazines, etc); verbal discussions or presentations with foreign nationals; hand carrying or shipments of items outside the U.S. or to foreign nationals within the U.S.; mailing, faxing, emailing items outside the U.S. or to foreign nationals within the U.S.; and understanding the definition of a foreign person and the proper procedure to obtain clearance for visits to NASA facilities.

The contractor currently is required to operate, maintain, and update the MSFC Center-wide UNITeS Export System (CUES) a web based application system that collects information that is used to track the number and type of export control activities that have occurred on the UNITeS contract in a given period (currently monthly). This information is delivered to NASA on a monthly basis to fulfill contractual requirements. To understand the contractor's requirements, the CUES User Guide, *MSFC Center Wide Unified Export System Users Guide*, is provided for review.

The UNITeS *Export Control Plan* is provided for information on what is expected of contractors in support of NASA export control. The requirements for Russia IT Services, which have special procedures related to export control, are included in the UNITeS Export Control Plan.

2.5.4 UNITeS Emergency Management

The NICS contractor will be collaborating with MITS for MSFC's Continuity of Operations (COOP). While the MSFC COOP will be led by NASA, in conjunction with the MITS contractor, the NICS contractor will be fully responsible for any related COOP tasks required by the NICS PWS.

This section describes how COOP is performed at MSFC currently under UNITeS, and can be used as an example for other center specific COOPS The NICS contractor will only be responsible for the related services that NICS provides that a center may need for COOP, e.g. related to communications.

UNITeS currently provides Continuity of Operations Plans (COOP) planning for MSFC. COOP planning refers to the internal effort of an organization, such as a branch of government, NASA

center, or contractor, to assure that the capability exists to continue essential operations in response to a comprehensive array of potential operational interruptions. While much of the renewed impetus for COOP planning focuses on responding to potential attacks, the highly decentralized nature of the NASA Centers suggests that all but the most widespread interruptions are unlikely to disable NASA as a whole. Nevertheless, localized operational interruptions that could necessitate the activation of a COOP at each NASA Center might include routine building renovation or maintenance, mechanical failure of heating or other building systems, fire, inclement weather, or other acts of nature. Other events that may interrupt NASA's activities include failure of information technology (IT) and telecommunications. The purpose of COOP planning is designed to ensure:

a. Safety and well-being of employees, visitors, and the public;
b. Essential functions and activities are conducted without unacceptable interruption
c. Normal operations are resumed as quickly, safely, and efficiently as possible.

The contractor is responsible for including in contingency planning:

a. Plan responsibility and scope
b. Emergency telephone numbers
c. Building and occupant information
d. Procedures for periods when facilities are closed
e. Communications
f. Mail delivery
g. The staffing of a command center team of employees and appropriate staff to participate and support in COOP activities for the CIO and MSFC/MAF Centers for LAN and WAN services *(Note: This is the key component NICS supplies for MSFC, example of what other centers are likely to request).*

The UNITeS COOP, which is not available for distribution, identifies essential matters to be considered in developing an effective COOP plan in support of the CIO pertaining to Local Area Network and Wide Area Network services (*Note: This is the key component NICS supplies for MSFC, and is an example of what other centers are likely to request).* These matters include the following:

a. Identification of all essential activities and functions
b. Identification and protection of vital records, systems, and equipment
c. Determination of succession and delegations of authority
d. Identification and preparation of alternate work sites
e. Identification and training of a team of employees to perform essential activities in an emergency
f. Development of a system of warning to alert employees of potential threats and what to do in an emergency

g. Development of a system for identifying the location and status of employees following an emergency
h. Development of ways to communicate with contractors' own employees

The UNITeS COOP is written in accordance with the following directives:

a. HSPD 5 – *Management of Domestic Incidents*
b. HSPD 8 – *National Preparedness*
c. MPR 1040.4 - *Continuity of Operations (COOP) Planning*

2.6 UNITES SAFETY, HEALTH, AND ENVIRONMENTAL (SHE) MANAGEMENT

2.6.1 UNITeS Safety

The contractor maintains a Safety, Health, and Environmental Awareness program throughout the contract, implementing safety awareness and training for employees, tracking close calls, lost time accidents, and OSHA recordable events. The contractor conducted regular assessments of assigned buildings and vehicles, capturing findings and tracking corrective actions to completion.

The contractor's industrial safety, health, and environmental program incorporated the following Safety and Health Program Core Process Requirement (CPR) elements documented in MPG 8715.1:

a. Management commitment and employee involvement in the safety and health program
b. System and worksite hazard analysis
c. Hazard prevention and control
d. Safety and health training
e. Environmental compliance

The UNITeS safety activities include the following:

a. Conducting monthly safety meetings
b. Conducting monthly supervisor SHE inspections
c. Supporting the monthly SHE Committee meeting to include any SHE Subcommittees that they might be involved in
d. Attending any SHE related training that might be recommended from the employee training needs assessment located on the Supervisor Safety web page (SSWP)
e. Submitting a MSFC Form 4371 to this office monthly required by the DRD 974SA-002
f. Submitting a SHE Plan required by DRD 974SA-001. The safety activities listed above are required by MPR 8715.1.

Safety involves the preparation and implementation of health and safety policies and procedures in compliance with Occupational Safety and Health Administration (OSHA), NASA, and MSFC standards and requirements. This element includes safety inspections and surveys, safety and health meetings, and maintenance records and reports of occupational injuries and illnesses.

NASA's Safety and Health Program responsibility starts with senior management's role of developing policies and providing strategies and resources necessary to implement and manage a comprehensive safety and health program. The NASA Safety and Health Program is executed by the responsible Mission Directorate Associate Administrators, Center Directors, Office of Safety and Mission Assurance (OSMA), component facility managers, safety managers, project managers, systems engineers, supervisors, line organizations, employees, and NASA contractors.

In general, the success or failure of NASA's safety and health efforts can be predicted by a combination of leading safety and health indicators (e.g., the number of open vs. closed inspection findings, awareness campaigns, training metrics, progress towards safety goals/objectives, the amount of hazard and safety analyses completed, and close calls) and its achievement measured by lagging safety and health indicators (e.g., the number of incidents involving injury or death to personnel, lost productivity [lost or restricted workdays], environmental damage, or loss of, or damage to, property). Like many successful corporations, NASA has learned that aggressively preventing accidents, mishaps, and close calls is good management and a sound business practice.

NASA undertakes many activities that involve high risk. The management of these risks is one of NASA's most challenging activities and is an integral part of NASA's safety and health efforts. NASA's goal is to maintain a world-class safety and health program by promoting an effective worksite-bases safety and health program.

The NASA Safety Program policy is provided in NPD 8710.2, *NASA Safety and Health Program Policy* requirements. Specific safety program requirements are delineated in NPR 8715.3, *NASA General Safety Program Requirements*. Specific health program requirements are delineated in NPD 1800.2, *NASA Occupational Health Program*. Specific environmental requirements are delineated in NPD 8500.1, *NASA Environmental Management.*

2.6.2 UNITeS Safety Performance

During UNITeS performance, the industry Lost Time Incident Rate (LTIR), against which UNITeS performance comparisons were made, continued to decline. The UNITeS safety related semi-annual performance data is as follows:

Historical safety statistics for the UNITeS contractor are as follows:

a. Number of Lost Time Incidents (April 2004 thru March 2008): 3 (06/16/04, 3/1/07, & 3/22/07)

b. Number of OSHA Recordable Incidents (April 2004 thru March 2008): Five (5) (09/20/07)
c. Total Quarterly Hours Worked:
   2004 = 1,610,640
   2005 = 2,261,931
   2006 = 2,271,534
   2007 = 2,347,956
   2008 = 531,722 (estimated)
d. Total Hours Worked: (04/01/04-03/31/08): 1,610,640 + 2,261,931 + 2,271,534 + 2,347,956 + 531,722 = 9,023,783
e. Annual Industry Average LTIR (Days Away, Transfer, and Restriction) for NAICS Code 541513 (2006): 0.30
f. Annual Industry Average OSHA Recordable Case Rate for NAICS Code 541513 (2006): 1.00
g. UNITeS LTIR: 0.0
h. UNITeS OSHA Recordable Case Rate: 1 x 150,000 / 1,680,623 = 0.089

2.7 UNITES FACILITIES MANAGEMENT

Facilities Management involves the establishment and maintenance of a uniform process for managing the use of assigned facilities. UNITeS personnel occupy onsite space at MSFC in 12 buildings; however this is for the entire UNITeS scope of work. The space currently utilized by UNITeS which is applicable to NICS on site at MSFC is as follows:

a. Approximately 68 offices in Building 4207
b. Approximately 990 square feet of lab space in Building 4207 for the Enterprise Network Management Center (ENMC)
c. Approximately 2,290 square feet of lab space in Building 4207 for the Network Operations Support Lab (NOSL)
d. Approximately 27,070 square feet of near site office space (e.g. Bradford Drive) is leased by the contractor to support UNITeS/NISN.
e. UNITeS available space for NISN gateways and Customer Service Representatives (CSRs) is distributed across all NASA Centers is documented in the *NISN Gateway and CSR Facilities Table*.

The following is the floor space at GSFC in support of NISN, less the gateway and CSR offices:

Category/Location	Office Space	Technical Space	Lab Space	Miscellaneous Space
Building 3		4,307	1,274	1,324
Building 13		230		
Building 14	5,605	21,042		196
Building 25	156		1,842	
Building 28	561	2,810	532	1,953
Building 32		3,065		

Building 18	1,050			
Off-Site Space	4,005			
Totals	**11,377**	**31,454**	**3,648**	**3,473**

2.8 UNITES QUALITY ASSURANCE AND MANAGEMENT

UNITeS quality assurance and management provides for the continued certification of the IT services for ISO 9000 certification. The NICS contractor will be adding additional certification for ISO 20000 as required by NICS PWS 2.9.

2.9 UNITES CONTRACT AND SUBCONTRACT ADMINISTRATION

UNITeS contract administration includes all contract and subcontract administration functions and activities required in performance of the contract. A listing of UNITeS subcontractors supporting Section 3.0, Agency-wide Information Services, of the UNITeS contract is presented below. This listing is exclusive of UNITeS subcontractors supporting UNITeS PWS Section 4.0, IEMP Integration Services, and PWS Section 5.0, MSFC Information Services.

UNITeS contract administration provides for a single point of contact (along with necessary supporting staff) that has been provided contractual authority by the prime contractor to interface directly with the UNITeS Contracting Officer, prepare comprehensive proposals associated with additional in-scope effort requested by the Contracting Officer, and to execute bilateral contract modifications on behalf of the UNITeS contractor. This organization is also tasked with ensuring that all required documentation deliverables are provided in accordance with the content and schedule requirements delineated in the Data Procurement Document (DPD).

UNITeS subcontract administration provides for a single point of contact (along with necessary supporting staff) that has been provided authority by the prime contractor to interface directly with the UNITeS Contracting Officer for the purposes of executing subcontract agreements with firms considered necessary to augment the workforce of the prime contractor and to meet small business subcontracting goals contained within the prime contract. This organization also prepares and submits to the Contracting Officer comprehensive subcontract consent packages prior to execution in accordance with contract requirements.

2.9.1 UNITeS Subcontracts in Support of NISN

The following table defines the UNITeS subcontractors currently supporting UNITeS PWS section 2.0, Program Management and UNITeS PWS 3.0, Agency-wide Information Services, subset NISN.

Type of Effort	Company	UNITeS PWS Section	Sub-Contractor or Vendor
EA, Strategic Planning, Customer Relations management	Booz Allen Hamilton, Inc.	3	Sub-Contractor
Network Services, Telecommunications	Honeywell Technology Solutions, Inc.	3	Sub-Contractor
Network Ops, Data Center Operations, Customer Support	InfoPro Corporation	3	Sub-Contractor
Satellite/Network Services	Marshall Communications	3	Vendor
Help Desk Ops, Customer Survey, Customer Support	Metters Industries, Inc.	3	Sub-Contractor
Professional Consulting Services for IEMP, Application Projects, WAN Services	Oakwood University	2/3	Sub-Contractor
Network & Circuit – Russia Services	Synterra	3	Vendor
Network Services	Systems Integration/Simulation & Modeling (SIM&S)	3	Vendor
Network & Circuit Services	TKC Communications	3	Vendor
IT Computer Services – Russia	TechTrans International	3	Vendor

2.10 UNITES WORK LOAD INDICATORS

2.10.1 UNITeS Contract Direct Hours

The table below, UNITeS PWS 2.0 Direct Hours FY07, depicts the direct labor hours expended in FY07 and FY08 for the services provided by UNITeS for PWS 2.0 Program Management. The labor hours include regular time, overtime, temporary labor, subcontract labor, and corporate interdivisional transfer labor. It should be noted that the hours for PWS Section 2 include all program/contract related labor for the entire scope of UNITeS activities and, therefore includes items and level of effort that are not being consolidated into NICS and instead are part of MITS and EAST.

		Calendar 07	Calendar 08
UNITeS PWS	**UNITeS PWS Title**	**Approximate Total Hours**	**Approximate Total Hours**
2.1	Project Management	20,000	17,000
2.10	Quality Assurance	6,000	7,000
2.2	Strategic Planning and Evaluation	28,000	26,000
2.3	Financial Management	35,000	30,000
2.4	Contract Administration	10,000	11,000
2.5	Procurement	31,000	28,000
2.6	Asset Management	29,000	25,000
2.7	IT Security Program	15,000	15,000
2.8	Safety	3,000	3,000
2.9	Facilities Management	6,000	5,000

2.10.2 UNITeS Office Supplies

The UNITeS Office Supplies applicable cost (e.g. both Program Management and NISN) for office supplies for FY07 and FY08 are as follows:

a. UNITeS PWS 2.0 Office Supplies for FY07 and FY08 respectively is approximately $113,000 and $112,000.
b. UNITeS PWS 3.0 Office Supplies for NISN for FY07 and FY08 respectively is approximately $231,000 and $235,000.

2.11 APPLICABLE DOCUMENTS

The following is a listing of applicable documents for background and historical section 2.0 and the relevant location.

Located at the MSFC FOIA Office http://foia.msfc.nasa.gov/ (See section 1.5.1)

a. "*Unified NASA Information Technology Services (UNITeS)*" contract, NNM04AA02C
b. UNITeS Contract, Attachment J-1, *UNITeS Performance Work Statement (PWS)*
c. UNITeS Contract, Attachment J-2, *Data Procurement Document*
d. UNITeS Contract, Attachment J-3, *Wage Determination*
e. UNITeS Contract, Attachment J-4, *Performance Standards*

Located at the NODIS (http://nodis3.gsfc.nasa.gov)

a. NPD 1800.2, *NASA Occupational Health Program*
b. NPD 4100.1, *Supply Support and Material Management Policy*
c. NPD 4200.1, *Equipment Management*
d. NPD 4300.1, *NASA Personal Property Disposal Policy*
e. NPR 4100.1, *NASA Materials Inventory Management Manual*
f. NPR 4200.1, *NASA Equipment Management Procedural Requirements*
g. NPR 4200.2, *Equipment Management Manual for Property Custodians*
h. NPR 4300.1, *NASA Property Disposal Procedural Requirements*
i. NPD 6000.1, *Transportation Management*
j. NPR 6200.1, *NASA Transportation and General Traffic Management*
k. NPD 8500.1, *NASA Environmental Management*
l. NPD 8710.2, *NASA Safety and Health Program Policy Requirements*
m. NPR 8715.3, *NASA General Safety Program Requirements*
n. NPR 9250.1, *Property, Plant, and Equipment and Operating Materials and Supplies*

Located at: MSFC Directives:
(https://repository.msfc.nasa.gov/directives)

a. MPR 1040.4, *Continuity of Operations (COOP) Planning*
b. MPR 8715.1, *Marshall Safety, Health, and Environmental (SHE) Program*

Located at the FAR: (http://www.arnet.gov/far)

a. Federal Acquisition Regulation, Part 45, *Government Property*

Located at the NFS:
(http://www.hq.nasa.gov/office/procurement/regs/nfstocA.htm)

a. NFS 1808.1100, *Leasing of Motor Vehicles*
b. NFS 1851.202, *Contractor Use of Interagency Fleet Management System (IFMS) Vehicles*
c. NFS 1852.223-76, *Federal Automotive Statistical Tool Reporting*
d. NASA FAR Supplement, Part 1845, *Government Property*

Located at NASA Forms:
http://server-mpo.arc.nasa.gov/Services/NEFS/Home.tml

a. NASA Form 1759, *Vehicle Justification*

Located at the US House of Representatives (http://thomas.loc.gov)

a. Energy Policy Act of 1992

Located at the Executive Orders:
(http://www.archives.gov/federal-register/executive-orders/)

a. E.O. 13149, *Greening the Government through Federal Fleet and Transportation Efficiency*

Located at the OMB (http://www.whitehouse.gov/omb/circulars)

a. OMB Circular A-11, Exhibit 300

Located at the Homeland Security Presidential Directives:
(http://www.dhs.gov/xabout/laws/editorial_0607.shtm)

a. HSPD 5 – *Management of Domestic Incidents*
b. HSPD 8 – *National Preparedness*

Located at Other Documents, B&H Applicable Documents
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. *Management Information Control (MICS), Procurement Purchase Procedures User Operations Guide*, (MICS_2i_Procurement_UOG.doc)
b. *Management Information Control System (MICS) Accounts Payable User Operations Guide*, (MICS_2i_AP_UOG.doc)
c. *Management Information Control System (MICS), Project Control User Operations Guide,* (MICS_2i_PC_UOG.doc)
d. *Management Information Control System (MICS), Property User Operations Guide*, (MICS_2i_Property_UOG.doc)
e. *Management Information Control System (MICS), Purchase Requisition (PR) User and Operations Guide (UOG)*, (MICS_2i_PR_UOG.doc)
f. *Management Information Control System (MICS), User and Operations Guide (UOG), Purchase Requisition (PR) Funding Process*, (MICS_2i_Fund_UOG.doc)
g. *Management Information Control System (MICS), User Operations Guide,* (MICS_2i_UOG.doc)
h. *MSFC Centerwide Unified Export System (CUES) Users Operations Guide,* (CUES_UOG.doc)
i. *N-PROP Quick Reference Guide*, (N-PROP_QRG_V4.doc)
j. *NISN Gateway and CSR Facilities*, (NISN Gateway and CSR Facilities.xls)
k. *NISN Procurement Metrics 12-08,* (Procurement Metrics 12-08.ppt)
l. *NISN UNITeS Auto-Create MICS PRs,* (Create MICS PR.ppt)
m. *Reporting Movement of UNITeS Controlled Property Procedures, SOP 1B219,* (1B219 Reporting Movement of UNITeS Controlled Property User Responsibilities.doc)
n. *Shipping UNITeS Property Procedure,* (2100-2004 Shipping Procedure.doc)
o. *UNITeS Export Control Plan,* (Final UNITeS Export Control Plan.doc)
p. *UNITeS Mapping To New Procurements*, (UNITeS Mapping To New Procurements.doc)
q. *UNITeS MICS Sample Cost Reports,* (UNITeS MICS Sample Cost Reports.doc)
r. *UNITeS NISN Vehicle List,* (UNITeS NISN Vehicle List.xls)
s. *UNITeS Receipt of Property Procedure,* (2100-2003 Receiving Procedure .doc)
t. *UNITeS Russia Services Shipping Instructions*, (Shipping Instructions[1].doc)

3 UNITeS NISN ENTERPRISE SERVICES

MSFC has been delegated the primary responsibility for NASA wide area network services, NISN Project. NISN project management is located within the CIO at MSFC. NISN contains two overarching services, Mission Network and Corporate Network. Mission Network operational control is located within GSFC's CIOs Information Technology and Communications Directorate and is supported by both the UNITeS and MOMS contracts. Corporate Network operational control is located within MSFC's CIO and is supported by the UNITeS contract. The two contractors provide customer service, engineering, IT security, operations and administrative support for all NISN services. The following sections provide a brief outline of these services as provided by UNITeS and MOMS. For a full description of the services that are not within this section, refer to the NISN-001-001 *NISN Service Document*. Additionally, the equipment that will be consolidated from UNITeS and MOMS into NICS is located in RFP Attachments J-8, *Government Furnished Property*, and J-9, *Installation Accountable Government Property*. Section 3.16 provides a listing of additional applicable UNITeS and MOMS NISN documentation.

Key to the success of NISN is the successful request fulfillment process of Network Service Request. This process is supported by UNITeS customer service representatives, engineering and operations. The *NISN Service Request (NSR) Processing Procedure* describes the engineering and operations facing processes for NISN NSRS. UNITeS customer service representatives, engineering and operations, tightly coordinates the fulfillment of NSRs as approved by the NASA service owners. Section 3.15.3, NISN UNITeS Mission & Corporate Network Service Request, includes the UNITeS NSRs for FY08.

The NICS contract will consolidate the NISN services of today with the Center LAN services of today into a new definition of NISN as follows from the NICS PWS:

"The NICS contractor will implement and manage a single end-to-end service provisioning organization that combines and streamlines LAN and WAN communications services for both corporate and mission networks. Therefore, for purposes of this contract, NASA has expanded the NASA Integrated Services Network (NISN) program/project responsibilities to include all services defined in this PWS section."

With the NICS emphasis on ITIL and the I^3P seamless service delivery vision, it is envisioned that the existing NISN and Center LAN processes and standard operating procedures will need to be merged to reflect the new definition of NISN as well as industry best practices. Examples of items that are envisioned to be revised are the *NISN Service Request (NSR) Processing Procedure* and the *NISN Service Document*.

3.1 UNITES NISN CORPORATE NETWORK SERVICES

3.1.1 UNITeS NISN Internet Protocol Address Management (IPAM)

NASA IP Address Management (IPAM) includes the management of all Corporate, Mission, and project address space, NASA IP addresses, domain names, and Autonomous System Numbers (ASN) assigned to the NASA OrgID with the American Registry of Internet Names (ARIN) and DOTGOV.GOV. UNITeS currently manages the Agency IPAM system, assigns and delegates NASA IP resources for approved NASA use, and coordinates with the Regional Internet Registries (RIR). The IPAM system is the approved NASA enterprise system for IP address management, Domain Name Service (DNS), and Dynamic Host Control Protocol (DHCP), and is intended to ultimately be the only system providing these services across the Agency.

UNITeS provides the sustainment and operational support for the deployed enterprise IPAM system, while currently each Center organization manages, within the enterprise IPAM system, the IP resources assigned to that particular Center and the Center's related projects. NICS will combine these two activities into an enterprise IPAM (e.g. Agency IPAM and Center IPAM).

NISN registers NASA.GOV, SCIJINKS.GOV, and CentennialofFlight.GOV domain names and administers the Internet domain naming policies, conventions, and the domain name servers (DNS) within NASA. Sub-domain management is conducted by the assigned NASA Centers within the IPAM system. There were approximately 430/month DNS changes in the past year.
NISN typically executes approximately 2 ARIN actions per month. Currently, NASA is assigned approximately 93 Class B and 1325 Class C address blocks, located within 30 Autonomous System Numbers (ASNs) in the Agency.

3.1.1.1 UNITeS NISN IPAM Migration (IPAM) Project

UNITeS is currently performing an enterprise IPAM Project to migrate the entire agency to the enterprise IPAM. By the time the NICS contract is awarded, NISN and all Centers' institutional networks are expected to be migrated to the enterprise IPAM system. The enterprise IPAM Migration Project was initiated in FY07 to consolidate and standardize the management of all Corporate, Mission, and Project, NASA IP addresses, domain names, and Autonomous System Numbers (ASN) assigned to the NASA OrgID with the American Registry of Internet Names (ARIN) and DOTGOV.GOV. The IPAM Migration Project will be completed prior to NICS contract award.

The following document describes the current IPAM Migration Project:

a. *IPAM System Design Document*

3.1.2 UNITeS NISN Remote Access Services (RAS)

This service is the Client Virtual Private Network (VPN) that each Center LAN provides today. As such, UNITeS NISN does NOT currently provide this service. The following describes a typical Center RAS:

Many Centers allow employees to use a remote access capability to work from home, on the road, or when visiting other NASA Centers. Some examples of today's Center remote access systems are Microsoft Windows servers running point-to-point tunneling protocol (PPTP), Cisco VPN, Cisco dial-in servers for dial-up networking and Juniper SSL-based VPN appliances.

Each Center's description of Client VPN is provided in Section 4.0. It is the future goal of NICS to combine the individual Center Client VPN systems into a single agency Client RAS service. This project has not been approved by the OCIO governance as this time.

It should be noted that it is in Section 3.4.2 DCNSS, which NISN provides client VPN service to server administrators in the NASA Data Centers.

3.1.3 UNITeS NISN Network Timing Protocol (NTP) Service

Network Time Protocol (NTP) service is an Internet Protocol that is used to synchronize a computer's clock to a reference time source. The NISN NTP Service provides NASA users and IT management organizations with a Stratum 1 NTP time reference source, available to Center and projects that can in turn distribute it within the Center or project. The NISN NTP servers respond to host polls with Coordinated Universal Time (UTC) timestamps with no offsets for any time zones. The NISN NTP servers provide UTC which is adjusted for leap seconds.

The NISN NTP service consists of servers accessible via wide area routed data networks at Marshall Space Flight Center, Goddard Space Flight Center, and Ames Research Center. Hosts located on any trusted NASA network may use the service by pointing to one or more of these six (6) NISN NTP servers. The NTP servers are modules residing in the chassis of the GPS timing source at these three NISN backbone core locations. NISN does not provide user support for servers and applications using the NTP service.

3.1.4 UNITeS NISN Guest Network Services

UNITeS NISN does NOT provide Guest Network Services. Refer to the Center-specific sections of background and historical, Section 4.0 Center and Associated Component Facility Services. It is NASA's goal to establish a Guest Network standard that eventually all Centers will comply with.

3.2 UNITES NISN CORPORATE VOICE SERVICES

The UNITeS contractor has coordinated with GSA to provide oversight of voice services purchased through FTS2001 and now Networx. In this capacity the contractor is responsible for supporting NASA in the purchase of circuits from Networx.

3.3 RESERVED

Intentionally left blank

3.4 UNITES NISN CORPORATE DATA SERVICES

3.4.1 UNITeS NISN Corporate Routed Data

NISN provides NASA with a Corporate, non-mission critical, wide area network routed data service as part of Corporate Routed Data.

The two service performance categories for Corporate Routed Data are defined as Premium IP (PIP) and Standard IP (SIP) Corporate service. If customer requirements cannot be satisfied by these two service categories, they may be supportable under Custom Network services, section 3.4.3.

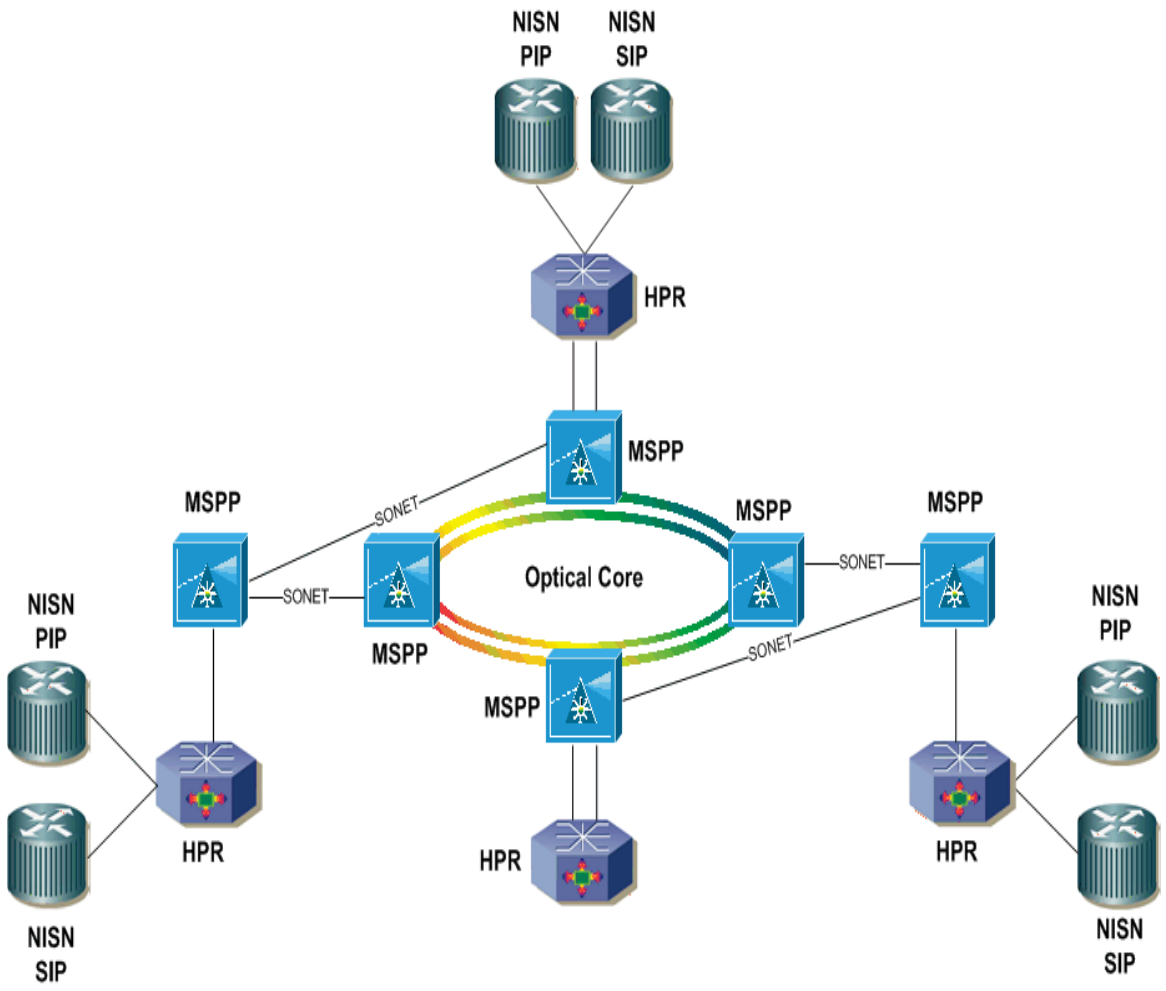
Currently with UNITeS, the service performance metrics for the two categories of domestic IP routed data service are as follows:

Service Category	Availability[1] (Percent)	Rest oral Time[3]	Coverage Period	Acceptable Packet Loss (Percent)	Round Trip Time[4]
Premium (PIP)	99.50	4 hr[3]	24X7	<1.0	<100 ms
Standard (SIP)	99.50	<24 hr[3,4]	6 a.m. Eastern Monday to 6 p.m. Pacific, Friday	1.0	<250 ms

1[+] These values apply only for those parts of the WAN service supported by the NISN mission services backbone infrastructure. These values do **not** apply to tail circuits unless the circuits/services were specifically ordered and supplied with diverse routing end-to-end.
2[♦] Round Trip Time (latency) is specified for data flow between domestic WAN nodes controlled and operated by NISN. Latency is a function of distance and carrier capabilities. User applications that are sensitive to latency shall be engineered to account for the upper limit round trip times specified in the above table.
3[→] These restoral times represent the time to restore service to the user and assume immediate access to the user's facility to repair/replace equipment if necessary.
4[*] The 24-hour restoral time results from the decreased priority given to standard service as compared to the other classes of service and from the fact that standard routed data service equipment is often a considerable distance from a NASA operating location.

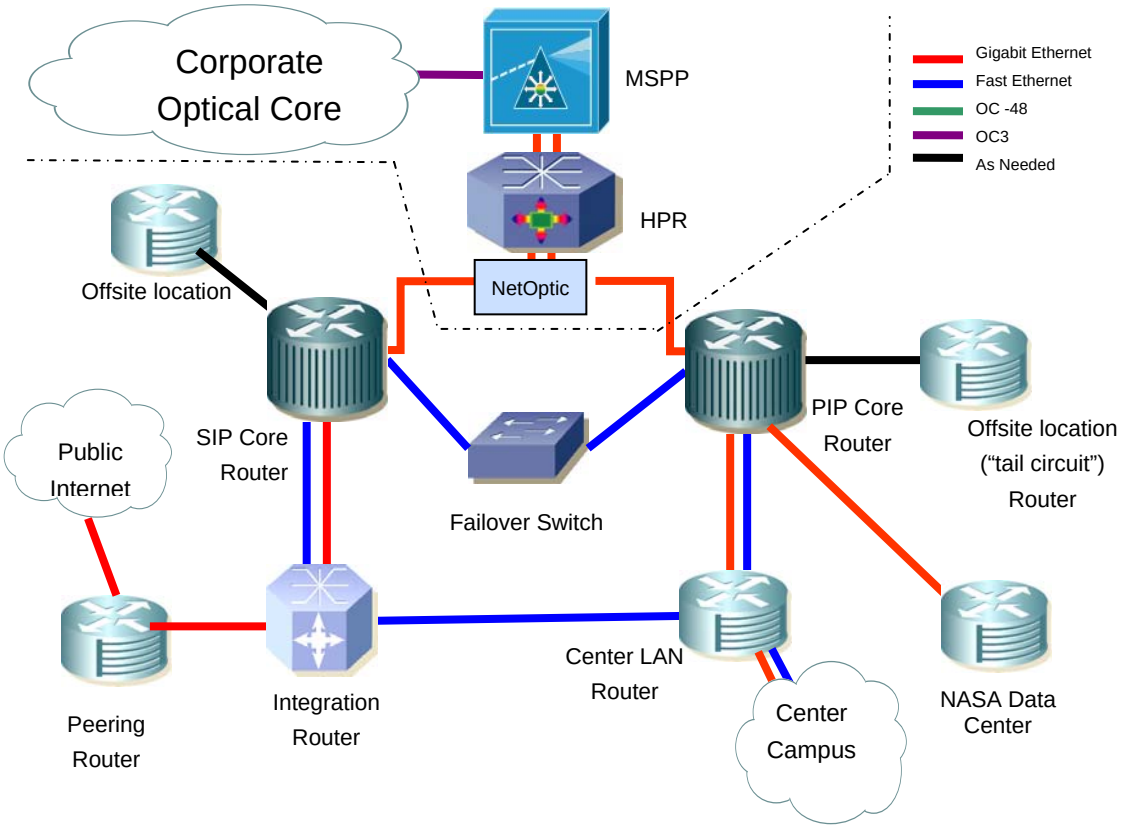
The figure below is an illustration of the NISN Corporate Routed Data Network

NISN Corporate Backbone and Routed Data Network Architecture:



The Service Demarcation Point for NISN IP Routed Data Services is the Local Area Network (LAN) interface of the Routed Data Service router. The LAN interfaces available include 10 Base T, 100 Base-TX, 100 Base FX, Gigabit (SX, LH, and ZX), and 10 Gigabit Ethernet. Several legacy interfaces that have been deemed End of Sales will continue to be supported until End of Life declarations are issued. The equipment list for the Corporate Network is located in the NICS RFP Attachments J-8, *Government Furnished Property*, and J-9, *Installation Accountable Government Property*. The figure below illustrates the Corporate NISN Routed Data WAN to LAN demarcations.

Routed Data WAN to LAN Demarcations:



NISN Corporate Routed Data circuits are included in Section 3.13, UNITeS NISN GSA Contract Integration.

NISN Corporate Routed Data supports several intra-domain routing protocols as follows:

a. Static, Routing Information Protocol (RIP)
b. Open Shortest Path First (OSPF)

NISN Corporate Routed Data supports inter-domain routing protocols as follows:

a. Border Gateway Protocol (BGP)
b. Multicast Border Gateway (MBGP)
c. DecNet across GRE Tunnels for specific project requirements

NISN works closely with customers to select a protocol consistent with both the customer's requirement and the common network architecture.

The following tables are the approximate Corporate Routed Data PIP and SIP server hardware count.

Corporate Routed Data PIP Service Hardware Count

Service Type	Vendor	Device Type	Model	Quantity
PIP	Cisco	Router	2691	3
PIP	Cisco	Router	2811	16
PIP	Cisco	Router	2821	3
PIP	Cisco	Router	3845	6
PIP	Cisco	Router	7300	1
PIP	Cisco	Router	2621XM	2
PIP	Cisco	Router	2651XM	4
PIP	Cisco	Router	7206VXR	2
PIP	Cisco	Switch	2950-12	1
PIP	Cisco	Switch	2950-24	2
PIP	Cisco	Switch	2950C-24	4
PIP	Cisco	Switch	2950G-24-E1	9
PIP	Cisco	Switch	2950G-48-E1	1
PIP	Cisco	Switch	3550-12G	1
PIP	Cisco	Switch	3550-48	13
PIP	Cisco	Switch	3560-24TS	1
PIP	Cisco	Switch	3560-48TS	10
PIP	Cisco	Switch	3560G-24TS	7
PIP	Cisco	Switch	3750G-24TS	1
PIP	Cisco	Router	6509	3
PIP	Cisco	Router	6509-E	5

Corporate Routed Data SIP Service Hardware Count

Service	Vendor	Device Type	Model	Quantity
SIP	Cisco	Router	1760	2
SIP	Cisco	Router	2500	1
SIP	Cisco	Router	2691	2
SIP	Cisco	Router	2811	27
SIP	Cisco	Router	2821	2
SIP	Cisco	Router	3825	2
SIP	Cisco	Router	3845	4
SIP	Cisco	Router	7206	1
SIP	Cisco	Router	7206VXR	7
SIP	Cisco	Router	7606	7
SIP	Cisco	Switch	2950-24	1
SIP	Cisco	Switch	2950G-24E1	6
SIP	Cisco	Switch	3550-12G	1
SIP	Cisco	Switch	3550-48	1
SIP	Cisco	Switch	3560-48TS	2
SIP	Cisco	Switch	3560G-24TS	3
SIP	Cisco	Switch	3750G-12S	1
SIP	Cisco	Switch	3750G-24TS	1
SIP	Cisco	Router	6509	9
SIP	Cisco	Router	6509-E	1

3.4.1.1 Routed Data Class of Service

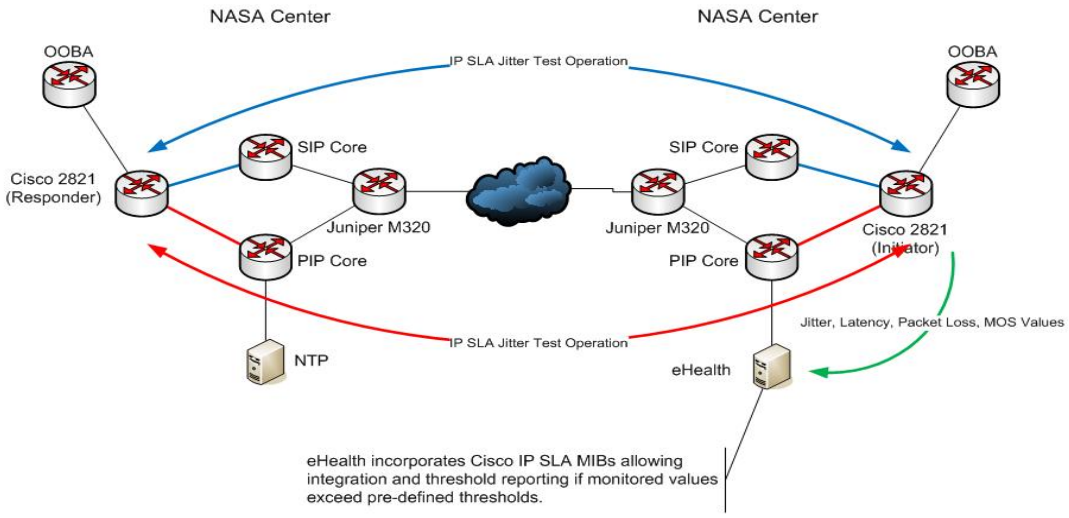
Under the existing Corporate routed data infrastructure, additional user systems are being developed which require support beyond the current service offerings. Video over Internet Protocol (ViIP) and Voice over Internet Protocol (VoIP) are examples of user class of services which need a guaranty of delivery of service to network sensitive applications.

A study has been completed which recommends the level and quality of service support needed at the edge of the network to support user requirements. The following implementation has been recommended and is proceeding for NISN approval and is expected to be in place by NICS contract award.

a. Strict priority queue policed and dedicated to TDM, VoIP bearer traffic and call-signaling traffic.
b. Video queue dedicated to real-time interactive video services.
c. Network control queue for Cisco and Juniper routing protocols.
d. Data queue for all remaining traffic categories. All terminations into the core network will be marked with the low drop priority as guaranteed delivery. Any utilization requirements above the agreed limits will be marked as high drop priority with best effort delivery.
e. Implement an "untrust" relationship on DSCP code-points between NISN demarcation and user community. NISN will mark code-points defined in the service delivery agreements.

An Internet Protocol Service Level Assurance (IPSLA) solution has been implemented on the routed data network. The solution provides NISN a glimpse into unidirectional latency and jitter values which are critical in calculating VoIP MOS scores. The IPSLA solution provides the ability to mark each packet with specific Class of Service (CoS) markings in order for the packet to be processed across the network in the appropriate queue. While these markings were not configured during the initial deployment, they are easily added to configurations.

The following diagram illustrates how IP SLA has been implemented:



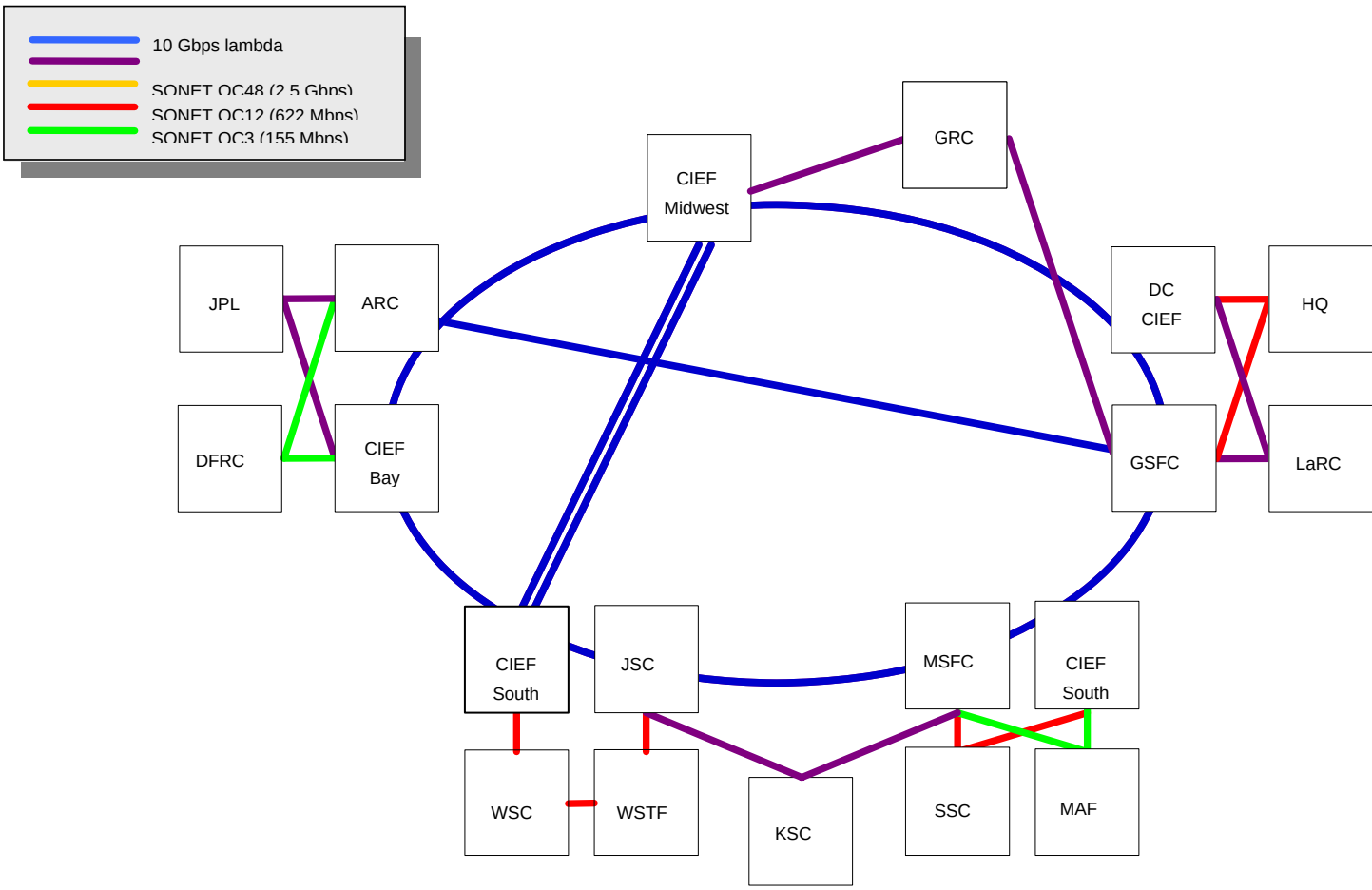
1

3.4.1.2 WANX Project

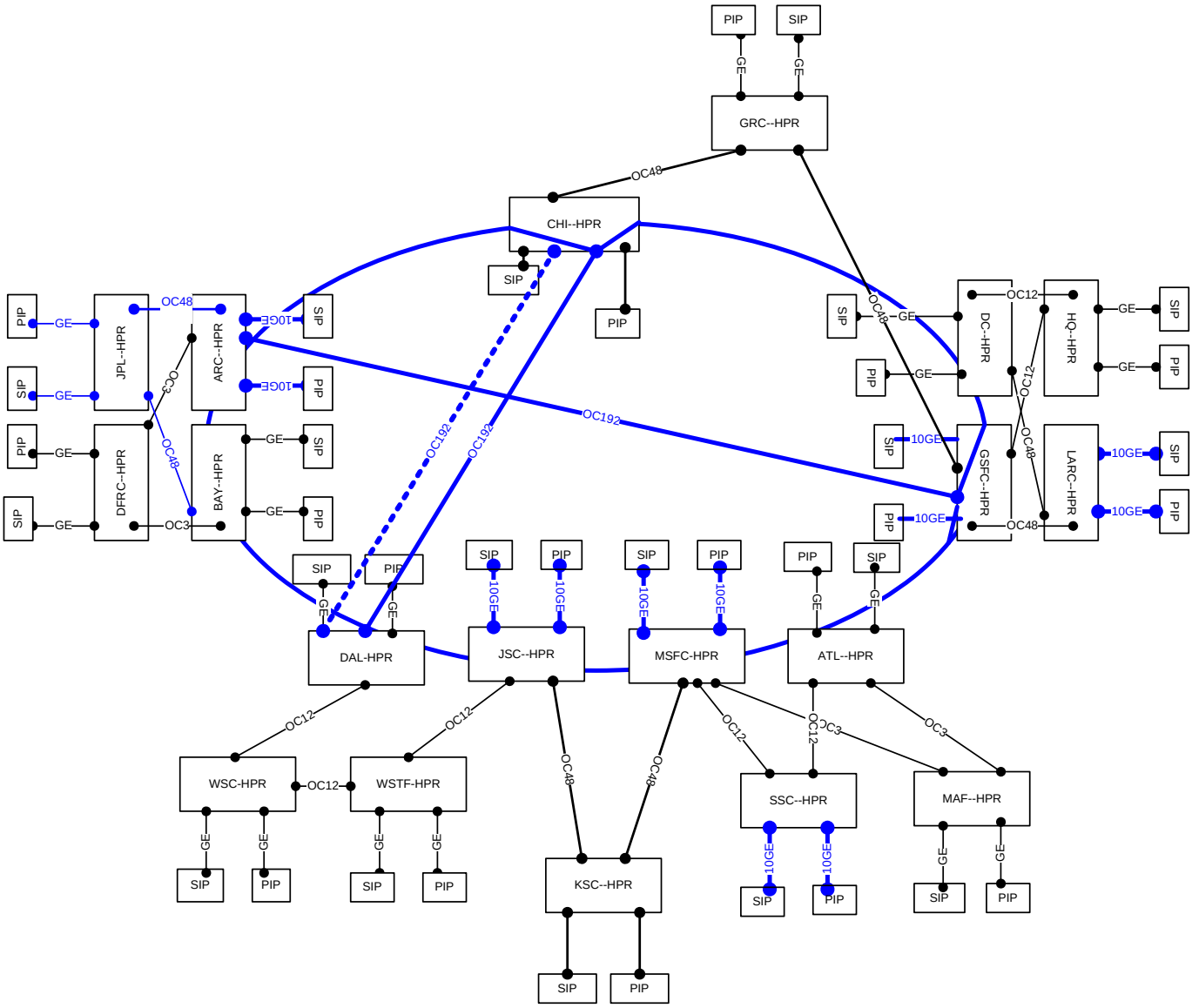
The UNITeS contractor will complete the WAN eXpansion (WANX) Project. WANX implemented the expansion of the NISN WAN core from OC48 (2.5Gbps) to OC192 (10Gbps), involving Corporate core backbone nodes at ARC, GSFC, JSC, and MSFC, as well as carrier independent exchange facilities (CIEF) in Atlanta, GA, Chicago, IL, Dallas, TX, San Jose, CA, and Ashburn, VA. The Corporate core architecture utilizes a Juniper Fast ReRoute (FRR) protection scheme to reduce risk of service disruption across the core. The Corporate regional architecture utilizes SONET signaling to reduce risk of service disruption to regional sites, including DFRC, GRC, HQ, JPL, KSC, LaRC, MSFC's MAF, SSC/NSSC, GSFC's WSC, and JSC's WSTF.

As with the previous backbone, the WANX backbone is designed with a pair of diverse, same speed circuits to each NASA Corporate core and regional location, with a 50% provisioning guideline, to ensure documented communications requirements can continue uninterrupted in the event of a single circuit outage. The contractor maintains adequate tools, policy, processes, and labor to monitor and maintain circuit diversity and 50% provisioning (subject to NASA funding for circuit expansions). The following documents describe the WANX project; *WANX Preliminary Project Plan* which will be complete prior to the start of NICS. The following figures depict the WANX changes to the backbone that will be in place at NICS contract award.

NISN Corporate Backbone at WANX Project Completion:



NISN Corporate Center PIP/SIP Demarcation at WANX Project completion:



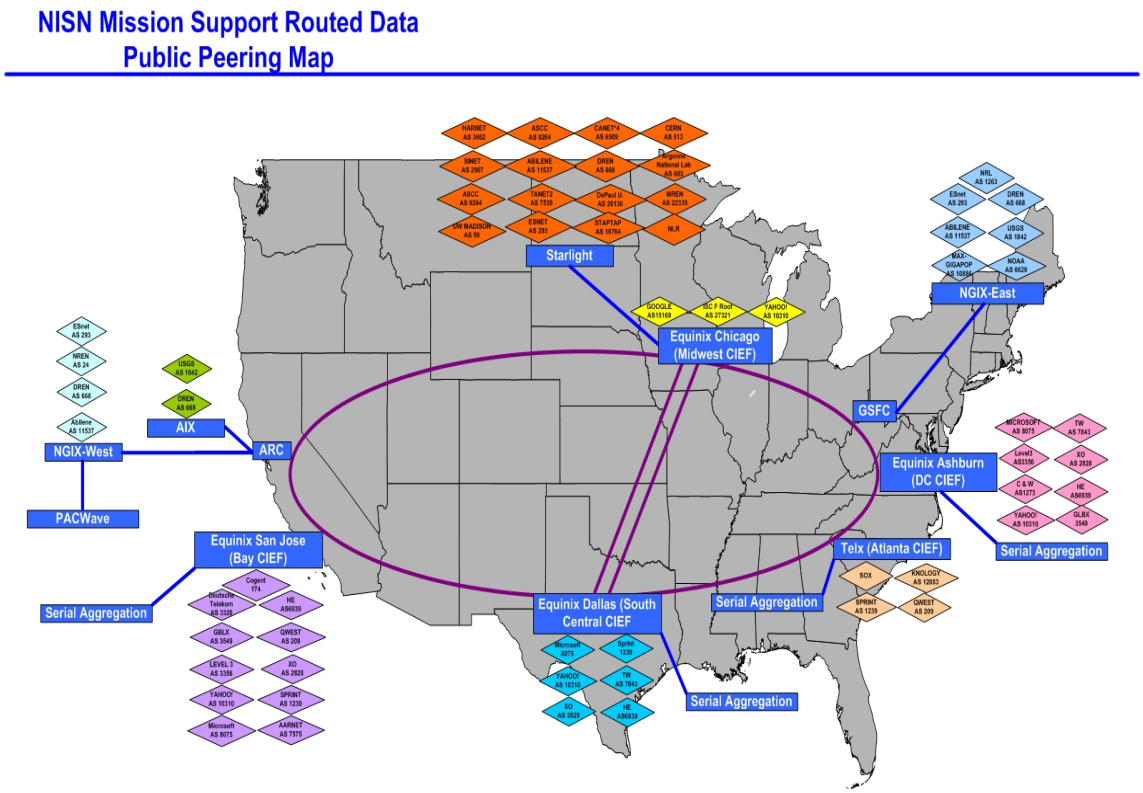
3.4.1.3 Corporate Routed Data Peering

The NISN Corporate Routed Data Peering provides for basic data networking connectivity using the IP suite. The NISN Corporate SIP service is the commodity Internet service that provides the Agency's link to the Internet. It provides basic universal Internet connectivity with lower performance guarantees or restrictions on acceptable use. Peering partners include both corporate and research networks dependent on NASA external peering requirements. The NISN Corporate SIP service is open to the public to enable access to publicly available NASA information sources such as World Wide Web services. The peering Points of Presence (POP) are located at five (5) Carrier Independent Exchange Facilities (CIEFs) plus peering equipment is also located at two NASA Centers, GSFC and ARC. The peering router, located in each CIEF, consists of a single Cisco 7606 terminated into the High Performance Router or HPR. Single Gigabit Ethernet cross-connects are made between NISN and each peering network. The hardware also has the ability to support 10 Gigabit Ethernet requirements with proper line-card installation.

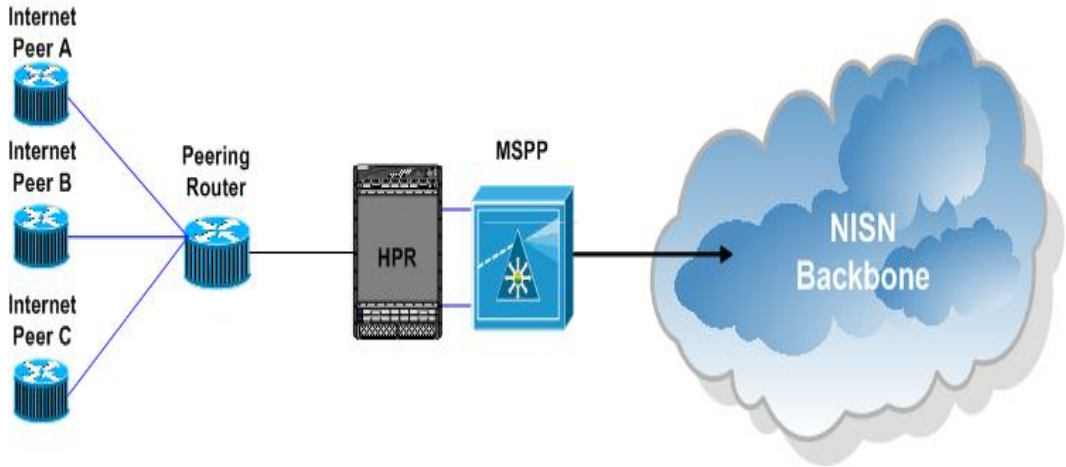
NISN's existing Corporate Routed Data SIP peering points are as follows:

Site	Provider	Location	Network Type
Atlanta CIEF	Telex	Atlanta Georgia Marietta Street	Corporate
Chicago CIEF	Equinix	Chicago Illinois Elk Grove	Corporate
Dallas CIEF	Equinix	Dallas Texas IBX Center	Corporate
San Jose CIEF	Equinix	San Jose South California IBX Center	Corporate
Washington CIEF	Equinix	Asburn Virginia IBX Center	Corporate
NGIX-East	University of Maryland	College Park Maryland Baltimore Avenue	Research
NGIX-West	Ames Research Center	Mountain View California Ames Internet Exchange	Research
Starlight	Northwestern University	Chicago Illinois North Lake Shore Drive	Research

An illustration of NISN's peering points of presence topology, less the research sites, is as follows:



The standard configuration is of a NISN CIEF Peering Site is as follows:



NASA has been directed by the Office of Management and Budget to comply with the Trusted Internet Connection (TIC) mandate. The TIC mandate requires all external network communications (e.g. peering points) to enter the NASA networks via an approved TIC, and to traverse a monitoring point managed by Department of Homeland Security (DHS) consisting of intrusion detection like system and Netflow collector. All monitoring equipment is maintained by the DNS with hands on support and connectivity into the network to be provided by NISN. The guidance provided by OMB can be found in *OMB Memorandum M-08-27, Guidance for Trusted Internet Connection (TIC) Compliance,* and *Draft_TIC_Conceptual Architecture.* NASA is in the pre-formulation stage of a TIC project to meet the OMB mandate. It is anticipated that there will be an IDIQ Task order for a TIC Project in FY10 but is not to be included in the initial contract value.

3.4.1.4 Corporate Routed Data IPv6

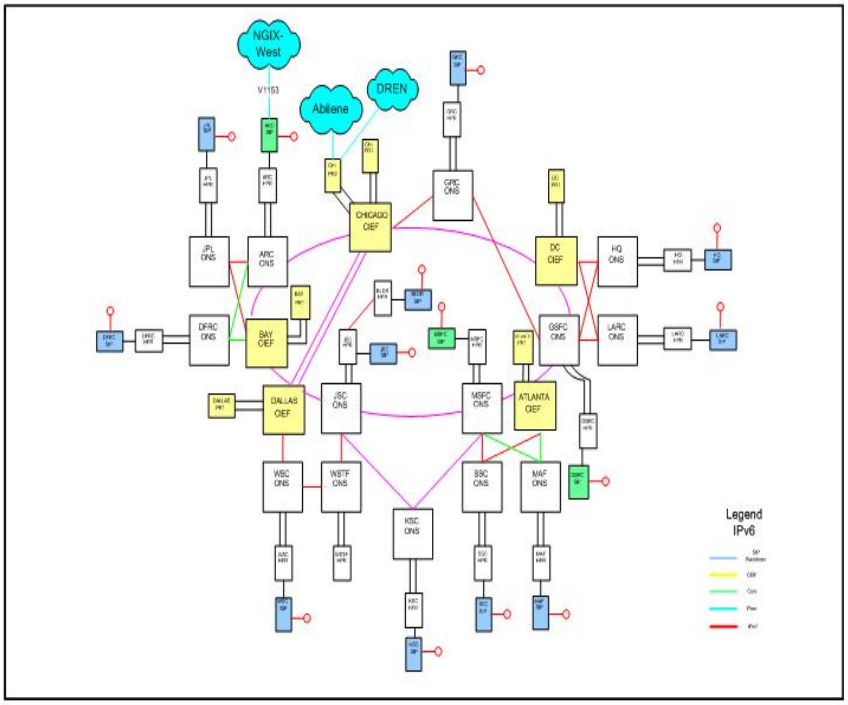
The Office of Management & Budget (OMB) had mandated that federal agencies demonstrate that they are IPv6 compliant by 6/30/08. NISN has implemented the following in response to this mandate:

a. Enabled IPv6 on all NISN SIP routers and Core routers to show that IPv6 traffic can be transported through an IPv6 network
b. Obtained the IPv6 address space needed by NISN to meet this mandate.
c. Enabled IPv6 on the standard corporate core routers of the NISN backbone.

NISN has the ability to support IPv6 trace route tests and pings between IPv6-enabled Iperf servers at all NASA Centers.

It should be noted that not all equipment that is on the NASA LANs are IPv6 compliant, however as the equipment is replaced the requirement is that the equipment be IPv6 compliant.

The figure below illustrates the NISN IPv6 implementation:

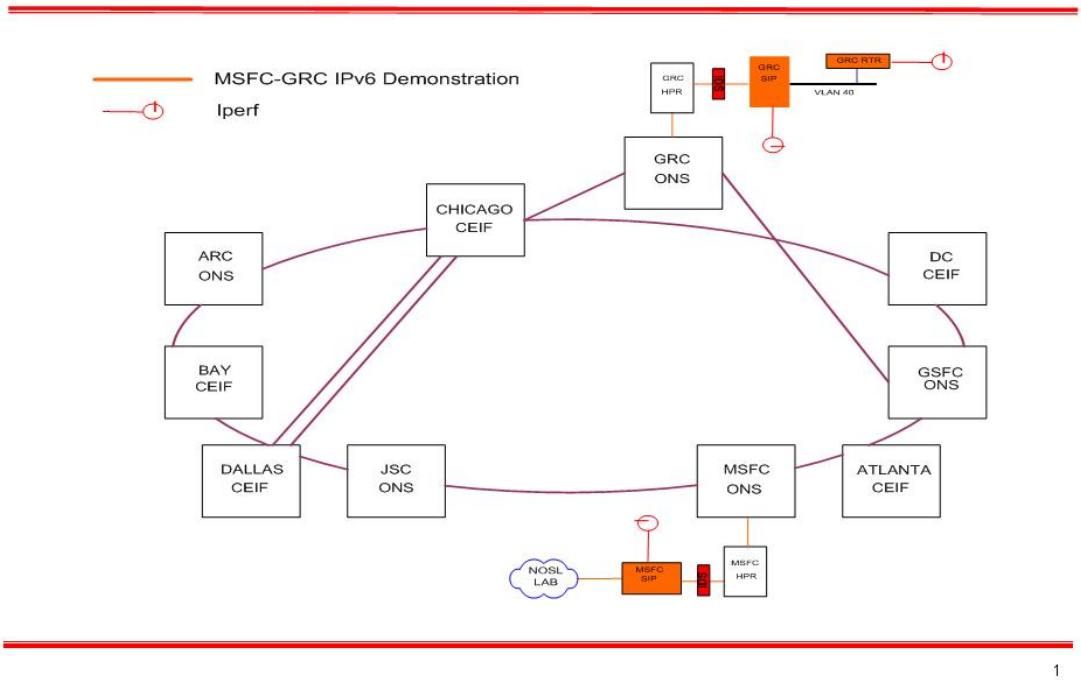


2/4/2009
Revision K

1

Enabling IPV-6 between NASA GRC and NISN routed data network addressed the ability to transmit IPv6 traffic through the network backbone out to another LAN. The design utilizes the IPv6 address space that will be allocated by IPAM to support GRC/NISN IPV6 configurations

IPv6 address space was also allocated to the Marshall Space Flight Center border router. One was a point-to-point between NISN and the MSFC border router. The second was a point-to-point between the MSFC border router and the NISN Operations System Laboratory. IPv6 was enabled on the Marshall border router incorporating the use of static routes between NISN MSFC SIP and MSFC. The implementation incorporated the use of Ipv6-enabled Iperf servers to do IPv6 ping and IPv6 trace route tests between the networks. Additionally, the implementation enabled IPV-6 between NISN, GRC, and MSFC across the NISN standard corporate routed data network. The implementation addressed the ability to transmit IPv6 traffic through the network backbone out to another LAN; in this case the NOSL and GRC test labs. Peering was enabled with both DREN via static routes. The following illustrates the GRC and MSFC IPv6 configuration:



IPV6 static routing is enabled on the internal core network allowing external peering with the DREN.

The remaining issue preventing the enabling of the IPV6 the protocol is the SNMPV3 IPV6 access control list. The hardware vendor has released the operating system image that supports the appropriate access control list. Prior to going operational, the system upgrade will be validated and tested in the NOSL and then the upgrade was moved to operations. Once this transition is complete, IPV6 will be enabled along with supporting external network routing protocol with external network peering partners. This work is anticipated to be complete prior to the start of NICS.

3.4.2 UNITeS NISN Data Center Networks

NISN provides Data Center Network and Security Services (DCNSS) for secure, highly available data center (centralized or distributed) networking infrastructure for computing systems and services that require a redundant infrastructure managed at an Agency level. High performance services, utilizing Juniper Netscreen ISG2000 or 5000-series firewalls deployed in a high availability (HA) configuration, are available at the following locations;

a. MSFC NDC
b. JSC NDC
c. ARC
d. GSFC
e. NASA Portal (Sungard) in Dallas, TX

In addition to these high performance services, NISN provides remote LAN services to each NASA Center for the Common Badging and Access Control System (CBACS).

Customers are able to tailor their services based on a grouping of service options and levels that meet their projects/programs requirements.

a. LAN Connectivity for Agency Wide Server Applications
    1) Switch Ports (10, 100, 1000Mbps)
    2) IP Address Assignment
    3) Domain Name Service (DNS)
    4) Server Network-based Load Balancing
b. Network Security Services
    1) Firewall Support
    2) Proxy Server Support
c. Reverse Proxy
d. WAN Connectivity
    1) Direct Connection to NISN WAN Services
    2) Encrypted Layer 3 Virtual Private Network (L3VPN) - see detail below
    3) Client-to-Network VPN Tunnels for System Administrator access to server resources (desktop client support NOT provided by NISN)

As an extension to traditional NISN Corporate WAN services, DCNSS extends the network support to NASA Data Centers and remote LANs by providing the following three distinct networks:

a. Private Network: Supports Data Center servers for Agency wide services not requiring Internet access
b. Public Network: Supports Data Center servers for Agency wide services intended to support services that extend beyond NASA to the Public Internet
c. Demilitarized Zone (DMZ) Network: Provides a secure path for traffic flowing between the Private and Public networks and to the NISN WAN

3.4.2.1 Layer 3 VPN (L3VPN)

NISN currently offers a network-to-network Layer 3 Virtual Private Network (L3VPN) service as a part of its Data Center Network and Security Services (DCNSS) suite, and is designed to support Agency server-based applications. This service provides point-to-point network-based VPN service to selected service delivery points, currently including ARC, GSFC, JSC, KSC, and MSFC, as well as the NASA Portal in Dallas. Other locations are implemented on an as-needed basis. This Layer 3 service provides an encrypted tunnel between two or more networks, and supports the FIPS 104-2 compliant encryption protocols. The devices used are Federal Information Processing Standard (FIPS) 140-2 compliant.

3.4.3 UNITeS NISN Custom Networks

Custom Network Services are provided to customers if the standard corporate services do not meet customer requirements. This service allows for networks comprised of different service performance categories to be installed at a customer location to provide increased reliability. Custom telecommunication and networking services are specifically designed and engineered to meet unique NASA programmatic requirements. Each program determines the unique attributes of the data distribution services in such terms as security, availability, redundancy, and features that provide the optimum trade-off between cost and program success. Examples of primary customers and the data that Custom Networks transports are:

a. International Networks
   Data Type: Data, Voice and Video

b. DRFC Infrastructure Support
   Data Type: Science Data

c. Multi-Channel Digital Television
   Data Type: Digital Video Flows

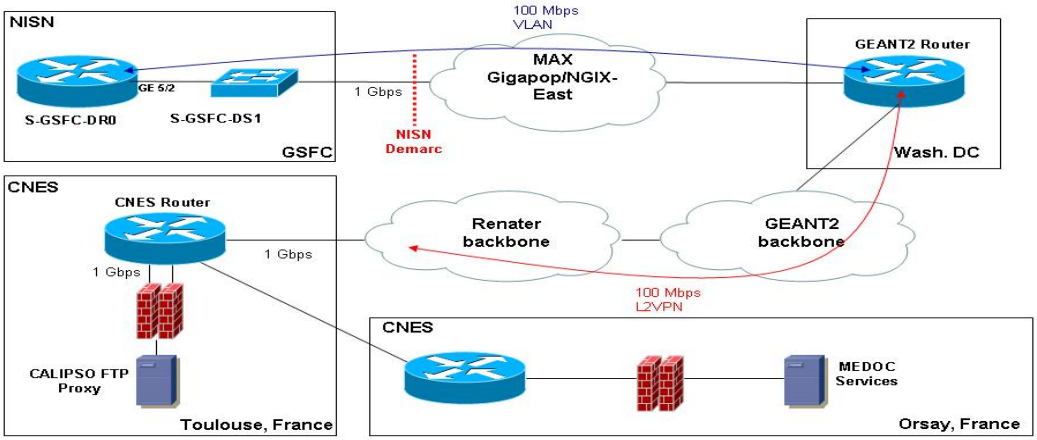
3.4.3.1 International Networks

International networks are those services that are provided to locations not within the Continental United States (CONUS). Vendors consider Alaska and Hawaii as international locations. Russia IT Services, which is an international service, is considered a separate NISN service (see section 5.1). International services can include data, voice, and/or video. International networks are currently provided in a range of speeds between 9.6Kbps to 52Mbps. Services traverse a combination of terrestrial and satellite technologies. Networks are engineered to a specific set of customer requirements.

Key International Space Agency Partners are as follows:

a. Canadian Space Agency (CSA)
b. Centre National d'Etudes Spatiales (CNES)
c. European Space Agency (ESA)
d. Japanese Aerospace Exploration Agency (JAXA).

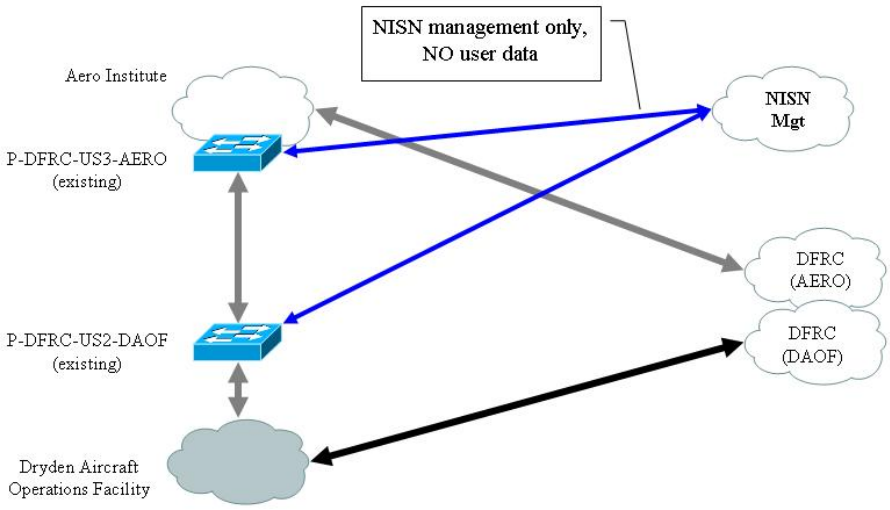
An example of international networks between GSFC and CNES supporting collaboration between NASA and the French Space Agency is provided below:



Traffic between CNES and NISN will move off of the fractional T-1 at GSFC and transit HPRENs*

3.4.3.2 DRFC Infrastructure Support

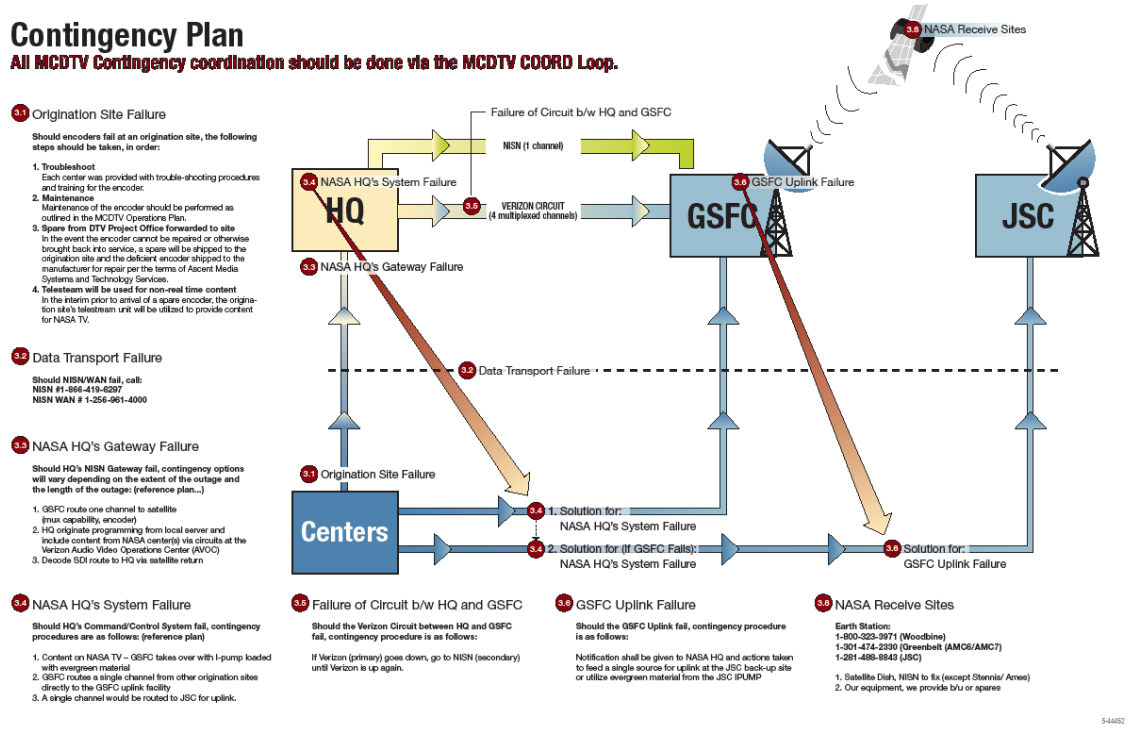
A NISN has implemented a custom network at the request of DRFC to support the local area network infrastructure. The requirement is provide minimum 40Mpbs (DS3, Metropolitan fiber) connectivity between DAOF (Dryden Aircraft Operations Facility) and Aero Institute in Palmdale, Ca. The customer requirements are to provide science network interface from DAOF to Aero Institute and back to DFRC. The following illustrates the DRFC Custom Routed Data Network:



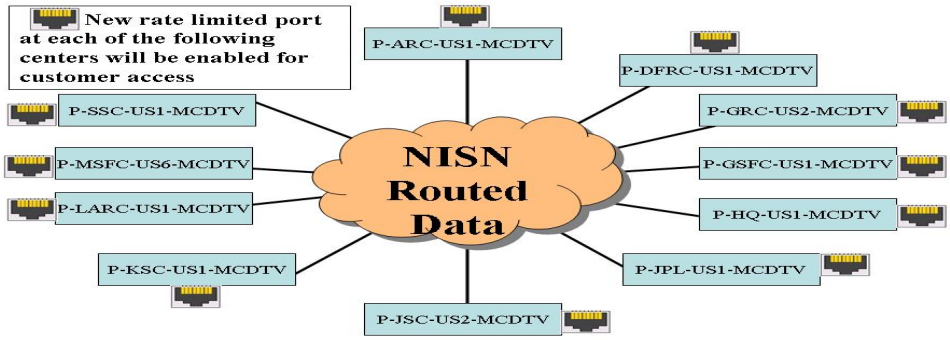
The science network traffic terminates into the DFRC LAN for subsequent DFRC campus routing and processing. Both the routed data equipment and circuits are procured by NISN with customer funding and is managed by the NISN Enterprise Network Management Center (ENMC).

3.4.3.3 Multi Channel Digital Television (MCDTV)

As part of the conversion of television to the digital format, NISN provides a custom network for MCDTV. The network supports the MCDTV Telestream project to provide the ability to transfer video files between centers. Eleven new Agency IP addresses were provided to customers for assignment to Telestream network equipment. As part of the implementation a single 2Mbs port was enabled to provide access at 10 centers and headquarters on the MCDTV switches. The following figure depicts the NASA MCDTV:

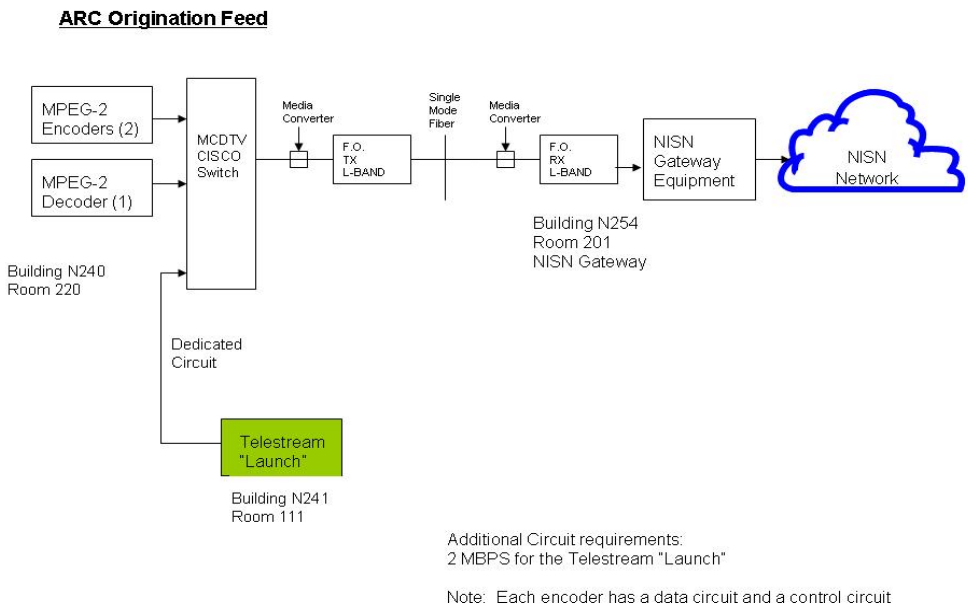


The following figure illustrates the MCDTV Corporate Custom Network service provided for MCDTV.



NISN provides the interface as transport into the network and manages the network switches as part of the service providing process being managed by the NISN Enterprise Network Management Center (ENMC).

The following depicts the ARC implementation of the Custom Network MCDTV equipment:



3.4.4 UNITeS NISN Firewall Services

The UNITeS NISN contractor manages day to day operations for Marshall Space Flight Center's institutional firewalls (e.g. both NISN and MSFC), UNITeS NISN DCNSS firewalls, and various MSFC project firewalls using Nokia hardware running Checkpoint, Cisco Pix/ASA firewalls and Juniper Netscreen firewalls. Duties include performing firewall policy changes, upgrades, patches, and maintenance and problem resolution on installed devices. The team researches, designs, implements and manages network security devices that include but are not limited to firewalls, virtual private networks and proxy servers that provide protection for the Marshall Space Flight Center's Private, Public, Agency, Project, NDC, NSSTC, NACC and other specified network infrastructures. The contractor will manage NCI specified firewalls as NCI deployments are completed.

3.4.5 UNITeS NISN Proxy Services

UNITeS NISN does NOT currently provide this service.

3.4.6 Reserved

Intentionally left blank

3.4.7 UNITeS NISN Layer 2 VPN Services

NISN operates an OSI Layer 2 Virtual Private Network (L2VPN) service as a complement to its suite of data transport services. The NISN L2VPN Service utilizes the same backbone infrastructure used to support Layer 3 data services, utilizing a NISN-managed MPLS core for separation, with switching equipment terminating into the NISN Backbone High Performance Router (HPR). A LAN extension from the NISN Gateway to the customer network is required. The L2VPN service is appropriate when the Customer requires transparent extension of LAN services between two or more physical locations. Unlike the NISN L3VPN service (under DCNSS), L2VPN does not provide data encryption. Use of L2VPN as a solution will be the decision of NISN based on established NISN and Agency policy. L2VPN service is offered only at established NISN backbone services locations, currently JSC, KSC, and MSFC.

The service demarcation point for the NISN L2VPN Service will be the Local Area Network (LAN) interface of the NISN L2VPN equipment. The LAN interfaces available include 10 Base T, 100 Base-TX, 100 Base FX, Gigabit (SX, LH, and ZX) Ethernet and 10 Gigabit Ethernet.

3.4.8 UNITeS NISN International Services

International telecommunications services are provided to facilitate Corporate and Mission communications with NASA's International Partner Agencies and their research facilities. This service provides transport of data, voice, electronic mail, and video. Table 1 illustrates those circuits which support the corporate network dedicated international circuit requirements.

Table 1 Corporate Network International Circuit List

NASA/ CONUS LOCATON	NASA/ CONUS CITY	NASA/ CONUS STATE	OCONUS/ INTERNATIONAL LOCATON	OCONUS/ INTERNATIONAL CITY	OCONUS/ INTERNATIONAL STATE
GSFC	GREENBELT	Maryland	ESA-ESTEC	NOORDWIJK	NETHERLANDS
GSFC	GREENBELT	Maryland	ESA-ESTEC	NOORDWIJK	NETHERLANDS
GSFC	GREENBELT	Maryland	ESOC	Darmstadt	GERMANY
GSFC	GREENBELT	Maryland	CSA-SS PROGRAM OFC	ST. HUBERT,QUEB	CANADA
GRC	CLEVELAND	Ohio	MD Robotics	Brampton, Ontario	CANADA
ESA = European Space Agency					
ESOC = European Space Operations Center					
NOAA = National Oceanic and Atmospheric Administration					
CSA-SS = Canadian Space Agency; Space Station					

International services are currently provided to the following international partners: European Space Agency (ESA), Canadian Space Agency (CSA), Center National d'Etudes Spatiales (CNES), and Japanese Agency (JAXA). Table 2 illustrates those circuits which support the Mission network dedicated international circuit requirements.

Table 2 Mission Network International Circuit List

Site	NASA/ CONUS CITY	NASA/ CONUS STATE	OCONUS/ INTERNATIONAL LOCATON	OCONUS/ INTERNATIONAL CITY	OCONUS/ INTERNATIONAL STATE
GSFC	GREENBELT	Maryland	ESA-ESTEC	NOORDWIJK	NETHERLANDS
GSFC	GREENBELT	Maryland	PF-RC	Fairbanks	Alaska
GSFC	GREENBELT	Maryland	PF-RC	Fairbanks	Alaska
GSFC	GREENBELT	Maryland	PF-RC	Fairbanks	Alaska
GSFC	GREENBELT	Maryland	PF-RC	Fairbanks	Alaska
Poker Flat	Poker Flat	Alaska	PF-RC	Chatanika	Alaska
GSFC	GREENBELT	Maryland	PF-RC	Chatanika	Alaska
U of Alaska	Fairbanks	Alaska	NOAA	Gilmore Creek	Alaska
GSFC	GREENBELT	Maryland	CENTRE NATL D'ETUDES	Toulouse	France
WSC	LAS CRUCES	New Mexico	Guam	Tanguisson	GUAM
WSC	LAS CRUCES	New Mexico	Guam	Tumon Bay	GUAM
GSFC	GREENBELT	Maryland	Santiago Tracking Station	Santiago/Peldehue	Chile
Goldstone	Ft. Irwin	California	Canberra/Telstra	Tidbinbilla	Australia
JPL	PASADENA	California	Canberra/Telstra	Tidbinbilla	Australia
NYC	New York	New York	Madrid	Madrid	Spain
GSFC	GREENBELT	Maryland	Madrid	Madrid	Spain
U of Alaska	FAIRBANKS	Alaska	KAKTOVIK OBSERVATORY	KAKTOVIK	Alaska
Gilmore Creek	Gilmore Creek	Alaska	PF-RC	Poker Flat	Alaska
GSFC	GREENBELT	Maryland	NOAA/Gilmore Creek	Fairbanks	Alaska
Gilmore Creek	Gilmore Creek	Alaska	PF-RC	Poker Flat	Alaska
GSFC	GREENBELT	Maryland	ASF, Univ of Alaska	Fairbanks	Alaska
GSFC	GREENBELT	Maryland	DLR GSOC MUENCHENER STR:20 82230	OBERPFAFFENHOFEN	GERMANY
GSFC	GREENBELT	Maryland	PASEO COLON	CORDOBA	ARGENTINA
JPL	PASADENA	California	ESOC	DARMSTADT	GERMANY
WSGT	LAS CRUCES	New Mexico	AUSTRALIAN TDRSS FACILITY	Dongara	W. Australia
JPL	PASADENA	California	Darmstadt	Darmstadt	GERMANY
JPL	PASADENA	California	Darmstadt	Darmstadt	GERMANY
JPL	PASADENA	California	CNES	Toulouse	France
JPL	PASADENA	California	CNES	Toulouse	France
JPL	PASADENA	California	GILMORE CREEK	Fairbanks	Alaska

WSC = White Sands Complex
WSGT = White Sands Ground Terminal
ESA = European Space Agency
ESOC = European Space Operations Center
CNES = Centre National d'Etudes Spatiales
PF-RC = Poker Flat Research Center

3.5 UNITES NISN CORPORATE COLLABORATION SERVICES

The contractor current provides new service fulfillment management, design, implementation for audio conferencing and Video Conferencing Services (VCS), Audio Conferencing (ACS), and Web Conferencing (WCS). Collaboration services are provided to all NASA Centers, Center associated component facilities, Headquarters, JPL, and to some non-NASA locations as designated by the NASA technical monitor. WCS will not be included in NICS.

For VCS the contractor provides maintenance, sustaining engineering; capacity management; and operation coordination.

For ACS and VCS the customer coordinates and monitors the delivery of these services from GSA.

3.5.1 UNITeS NISN Video Conferencing Service (VCS)

NASA VCS provides for the video conferencing needs of the Agency. The VCS service is coordinated through the UNITeS provided NASA Teleconferencing Center (NTC). The NTC consists of the enterprise VCS infrastructure, the VCS Room Packages, and the VCS reservation system. The following documentation provides additional technical detail on VCS:

a. *ViIP Overview Presentation*
b. *NASA Teleconferencing Services and ViIP Network Overview*
c. *Agency wide ViIP Initiative*
d. *ViTS over IP Services (ViIP) Migration Plan White Paper*
e. *NTC Brochure (Draft)*
f. *Collaboration Services- ViTS Rooms*

3.5.1.1 NISN VCS Enterprise Infrastructure

The contractor provides sustaining engineering for the VCS bridging infrastructure that interfaces to the VCS Room Packages delivered to the customers. The bridging infrastructure is capable of supporting multiple formats, utilizing bandwidths and resolutions ranging from 384kbps to 1.9 Mbps and from CIF to 720P High Definition (HD) as defined in H.320 and H.323 International Telecommunications Union (ITU) videoconferencing standards. These bridging services support ISDN to ISDN, ISDN to IP, and IP to IP. The contractor also provides a backup bridging service with the same performance and interoperability requirements via GSA. In support of VCS the contractor performs the following:

a. Provides for interactive point-to-point and multipoint conferencing.
b. Facilitates transmission and distribution of the video, audio, and graphics among the VCS locations participating in a conference.
c. Provides “Instant Video” capability that encompasses the contractor's total overall conferencing capability. The contractor provides the maximum number of endpoints that can participate in a single multipoint conference operating at 384 kbps for

Standard Definition (SD) video teleconferencing and at 1.9Mbps for High Definition (HD) video teleconferencing.

d. Obtains, via GSS, closed captioning services in compliance with Section 508 of the Rehabilitation Act of 1973.
e. Provisions teleconferencing bridging service for both ISDN and IP that utilizes International Telecommunication Union (ITU H.320 & H.323 standards based calls including, but not limited to, H.263, H.264, and H.239, Common Interface Format (CIF), 2CIF, 4CIF, and High Definition (HD) 720p video formats and G722, G728, Siren14, 22 audio formats.
f. Provides the ability to extend an active conference without advance notice.
g. Supports Continuous Presence for both SD and HD conferences. The contractor provides a minimum and maximum number supported for Continuous Presence in both a SD to SD, SD to HD and HD to HD conference.
h. Provides the capability for encryption to include Advanced Encryption Service (AES) based on ITU standards H.235 version 3 for ISDN and IP bridged calls. AES should be available for both SD and HD conferences.

The following documentation provides additional technical detail on VCS Infrastructure:

a. ViIP Configuration Document

3.5.1.2 NISN VCS Room Packages

In support of a request fulfillment for a VCS service, the contractor provides for the engineering and sustainment of various VCS room packages that are delivered to NASA Centers, Center associated component facilities, Headquarters, JPL and NASA designated non-NASA facilities. The various services are as follows:

a. Full Service Room Packages - Full Service packages are designed for large conference rooms capable of seating up to hundreds of users. Full Service packages provide permanent fixed capabilities such as dual video screens, multiple cameras, recording capability, individual mutable microphones, pop-up units for power and computer capabilities, and room lighting control, interface to LAN services, and room control panel. The ACS service owner recommends that these rooms be operated by a dedicated room operator.

b. Multimedia Room Packages - Multimedia packages are designed for large conference rooms capable of seating up to hundreds of users. Multimedia rooms provide permanent fixed capabilities such as dual video screens, multiple media inputs, recording capability, pop-up units for power and computer capabilities, and room lighting control, interface to LAN services, and room control panel. The ACS service owner recommends that these rooms be operated by a dedicated room operator.

c. Portable Room Packages – Portable systems provide capabilities such as dual video screens, multiple cameras, recording capability, individual mutable microphones, pop-up units for power and computer capabilities, and room lighting control, interface to LAN services, and room control panel. These packages are installed on a cart or movable equipment with interface to conference room power and LAN interfaces. These packages are designed for user-friendly operations and should not require a dedicated room operator.

d. Table Top Standalone Room Packages – Table top standalone systems are designed for one user. It provides capabilities such as video and audio conferencing. These table top systems are designed for user-friendly operation by the user alone.

e. VCS Room Operators – VCS provides as a service room operations for two VCS Room Packages; Full Service Room Package and Multimedia Room Package. This separately purchases service provides for a VCS room operator dedicated to the customer locations.

The following documentation provides additional technical detail on VCS Room Packages:

a. Example 1: ViIP NSR
b. Example 2: ViIP NSR
c. Example: Custom Full Service ViIP
d. Example: Custom ViIP Custom Multimedia
e. Example: ViIP Audio
f. Example: ViIP Roll-About
g. ViIP Certification for VCS Room Packages
h. ViIP Configuration Document

3.5.1.3 NISN VCS Reservation System

Key to the success of the NTC, the contractor supports the maintenance, sustainment and operations of a VCS Conference Reservation System (VRA). The VRA reserves both facility and bridging resources.

In support of the VRA, the contractor performs the following:

a. Submits reservation requests (up to one year in advance of the conference date) by phone, email, fax, or via a web-based schedule system.
b. Supports both PC and Macintosh platforms.
c. Provides the ability to input desired dates, times, and facilities to be used in a conference.
d. Provides notification of room and/or bridge availability.
e. Provides oversight necessary to avoid double-booking of facilities and bridging services.

The following documentation provides additional technical detail on VCS Reservation System:

a. *VoTs User Guide*
b. *NRS User Guide*
c. *VRA User Guide*
d. *ViTS ISDN Directory*
e. *VoTs Directory*
f. *VoTs and ViIP Statistics*

3.5.2 UNITeS NISN Audio Conferencing Service (ACS)

NASA ACS provides for the audio meeting and conferencing needs of the Agency. The contractor coordinates with GSA (e.g. Networx), for this service. In general, GSA provides for direct customer interaction and maintains the ACS infrastructure. The contractor monitors GSA performance and supports incident and problem management oversight of GSA. There are three services GSA provides:

a. Attendant Assisted Conference Service
b. Instant Meeting Conference Service
c. Standard International Dial-Out Service

A key part of the contactor's coordination with GSA is notification of NASA holiday/vacation periods. GSA is responsible for sending notifications to NASA customers reminding them to make note of holiday/vacation periods. GSA sends these notifications to ACS customers' ten (10) business days prior to Thanksgiving Day and ten (10) business days prior to Christmas Day.

The following documentation provides additional technical detail on ACS:

a. *VoTs User Guide*
b. *VoTs Directory*
c. *VoTs and ViIP Statistics*

3.5.3 Reserved

3.6 UNITES NISN CORPORATE MANAGEMENT AND OPERATIONS

3.6.1 UNITeS NISN Corporate Network Management and Monitoring

UNITeS provides for network monitoring and management for the NISN Corporate network. In performing these services the contactor captures and reports near-real-time network performance and utilization statistics. The NISN Corporate Network Operations Center, ENMC, is located at Marshall Space Flight Center (MSFC), Building 4207/Room 101, in Huntsville, AL. The ENMC supports many functions to include network monitoring and management. Typical manned

operating hours are 7x24x365. Current staffing consists of network analysts and helpdesk technicians.

Recently, the ENMC has been upgraded to facilitate tool/task reduction of duplication, consolidation, integration, and future monitoring requirements. To that end the ENMC staff provides the following:

a. Integrated Enterprise Network Management System (ENMS), Firewall, and IT Security Operations network enclaves into a single NOC.
b. Integrated System Administration, tape backups, firewall, and other general purpose network activities
c. Refocused integration efforts using existing toolsets to meet current and future requirements
d. Continued with in-depth analysis of several vendor platforms to enhance management and potentially reduce costs
e. Implemented DCN, integrated applications, and MSP if mission focuses on end-to-end monitoring
f. Implemented ITIL processes across NISN organization

The ENMC staff retired the following:

g. Redundant e-mail, tape systems, authentication, and NTP services
h. Juniper JUNOScope and Panavue

For a more complete understanding of this upgrade, refer to the following documentation:

a. Network Management Case Study Findings
b. ENMC Network Management System (NMS) Refresh CCB Presentation

For a full listing of the tools that apply to the ENMC refer to section 3.15.1.5 NISN Corporate Tools. For performance standards related to the ENMC refer to NICS RFP Attachment J-1 *Performance Work Statement* Appendix B, *Performance Specifications*.

3.6.2 Colaboration Management and Monitoring

The UNITeS contractor currently operates the NASA Teleconferencing Center (NTC) to manage and monitor the collaboration services. The tools used by this operations team consists of the enterprise VCS infrastructure, the VCS Room Packages, and the VCS reservation system.

3.6.2.1 Collaboration NASA Teleconferencing Center

The contractor staffs the NTC Monday through Friday, 6am-6pm, Central Standard Time. The NTC shall be staffed outside of these hours as requested by NASA. The NTC contractor staff performs the following functions:

1. Provides the interface between the users and providers of the Collaboration Services.
2. Maintains the Collaboration Services Facilities Directories to contain at a minimum: building, room, point of contact information, and facility conference name designation and dial number(s), and internet protocol address(es) (to conference directly with facility).
3. Processes reservations, schedule resources for video conferences, initiate VCS calls, and monitor call quality.
4. Operates VCS Reservation System, including account approval and reservation of facility and bridging resources.
5. Provisions and operate the VCS Bridging System.
6. Develops and maintain usage and service performance reports for the VCS.
7. Maintains and implement processes for activation of, and failover to, the GSA backup VCS bridging service.
8. Maintains integration and interoperability procedures with non-NASA VCS conferencing services, including but not limited to GSA/Networx, Defense Information Services Agency (DISA), and internet-based conferencing services.
9. Monitors VCS and ACS conferences held to conduct the planning, monitoring, and closeout of manned spaceflight missions.

3.6.2.2 Collaboration Maintenance

The contractor maintains the following:

a. Maintains VCS and ACS facilities, including associated hardware and software systems, room layout, video projection screens or monitors, audio equipment, interactive graphics and document sharing systems, and room operations panel.
b. Maintains the VCS Reservation System.
c. Maintains the VCS Bridging System.
d. Provides dedicated room operator support at locations designated by the COTR or designee.
e. Maintains interoperability between all VCS and ACS facilities provided under this contract.
f. Implements the VCS and ACS facility maintenance policies.
g. Provides on-site support, for those locations designated by NASA, and trouble isolation/escalation for VCS and ACS conferences held to conduct the planning, monitoring, and closeout of manned spaceflight missions.

3.6.2.3 UNITeS NTC Coordinate with GSA

The contractor NTC team coordinates with GSA on a daily basis for the three types of voice services (ACS) NASA has purchased as follows:

d. Attendant Assisted Conference Service
e. Instant Meeting Conference Service
f. Standard International Dial-Out Service

3.6.2.3.1 NISN NTC/GSA Attendant Assisted Conference Service

This service includes a Networx attendant on the call that provides the call out to each participant approximately ten (10) minutes prior to the scheduled call time and provides the announcement of each participant.

3.6.2.3.2 NISN NTC/GSA Instant Meeting Service

Instant Meeting service includes a two type of services as follows:

a. USA Instant Meeting Service -Conferencing that provides a customer subscribing to this service a toll-free number with separate leader and participant pass-codes. The subscription is available for activation of conferences twenty-four (24) hours a day, seven (7) days a week, regardless of holidays. The accounts are available to the participant for a minimum of six (6) months. All accounts are to be pre-set to provide notification to the account holder when their account has been used. All accounts allow a minimum twenty (20) participants for a minimum of eight (8) hours. The NTC staff is on stand by to handle any issues or support customers.

b. International Instant Meeting Service – Conferencing that provides both international and USA participation. This Global Access Toll/Toll Free provides to customers a toll free International phone number or a toll access in-country number that terminates on a conferencing bridge in the US. Global Access Toll/Toll Free (for scheduled conferences) which provides any conferencing users a local, in-country phone number (local toll or free phone) that they can dial from their respective location and are joined together on a common bridge platform. The NTC staff is on stand by to handle any issues or support customers.

3.6.2.3.3 NISN NTC/GSA Standard International Dial-Out

The Standard International Dial-out service provides the customer with the ability to dial-out to a non-domestic location allowing the addition of a non-domestic participant to an audio conference. The NTC staff is on stand by to handle any issues or support customers.

3.6.2.3.4 NISN NTC/GSA Special Missions Specific Service

Occasionally the NISN NTC/GSA operations team supports special Mission conferences. During the past year this special service was provided for approximately six manned spaceflight Missions, with an average duration of 20 days per Mission.

3.6.2.4 UNITeS NTC/GSA Provided Conference Reservation System

GSA provides to NASA a conference reservation system, containing specific details about their conference, which provides users the ability to submit reservation requests up to one year in advance of the conference date by phone, email, fax, or via an online schedule system. The UNITeS contractor provides a toll-free dial telephone number for use in scheduling reservations. The GSA online schedule system is compatible with both PC and Macintosh Platforms and information on the reservation system is made available as public domain on the NISN web site. The contractor uses this GSA provided system to allow the following:

a. Ability to monitor in-progress calls, provides technical support, and monitor conference quality.
b. Ability to support up to 350 NASA community users participating in one conference
c. Ability to conduct up to 70 simultaneous and independent conferences at any one time.
d. Ability to extend an ACS with no notice.
e. Capability to record and transcribe conferences as requested by the call leader.
f. ACS service performance requirements as follows:
g. Service availability of ≥99.50%
h. Time to restore bridging service (without dispatch): ≤4 hours
i. Time to restore bridging service (with dispatch): ≤8 hours
j. Time to restore bridging service during an in progress call: ≤15 minutes
k. Operator assistance response delay during an in progress call: ≤5 seconds
l. Mean time to respond to problems on an in progress call: ≤3 minutes
m. ACS account implementation for new requests: ≤30 minutes from receipt of request.

On-time provision of new services on dates agreed to by firm order commit date. The NTC staff is on stand by to handle any issues or support customers.

3.6.2.5 VCS Room Operator

The contractor provides VCS Room Operators at NASA direction. For this customer purchased service, the contractor provides the following support:

a. Scheduling VCS facilities and Bridges services as requested by the conference host.
b. Coordinating with other room operators to resolve any scheduling conflicts.
c. Monitoring and operating VCS conference sessions as directed by the conference host.
d. Interacting with other VCS room operators and the VCS bridging infrastructure operators to ensure the conference is conducted smoothly.
e. Reporting any facility issues to the NTC or designated location point of contact.

f. Reporting any VCS operational problems via the designated trouble reporting process.
g. Completing training as directed by the NTC.

3.6.3 UNITeS NISN Technical Field Support

The WAN currently has dedicated telecommunications gateway facilities that are the interfaces for WAN services into the NASA centers. These gateways typically contain the demarcation point for carrier circuits, center border routers, center switches, video teleconferencing equipment for Virtual ViTS Connections, and various test equipment. The following documents provide additional information on NISN Corporate Gateways:

a. *NISN Corporate Gateways Addresses*
b. *NISN Gateway and CSR Facilities*

3.6.3.1 NISN Clearances Needed for Gateways and ENMC

The contactor provides the following number of cleared personnel for the gateways:

a. Approximately 35 Gateway technicians cleared DoD Secret
b. Approximately 18 cleared DoD Secret and 2 TS ENMC staff
c. Additionally managers in both engineering and operations are cleared DoD Top Secret

3.6.4 UNITeS NISN Corporate Maintenance

The contractor supports NISN Corporate Maintenance with three types:

a. Make Operable: Emergency maintenance to bring the network back to operational
b. User/Customer Approved Maintenance: Pre-approved outage with user/customer to do maintenance on the equipment supporting their service.
c. Schedule Activities Maintenance: Pre-scheduled 10 day notice in advance, schedule outage to maintain equipment.

3.6.5 UNITeS NISN Corporate Services Scheduling

NISN Corporate Network uses the NISN Activity and Outage Posting and Notification System (AOPNS), an email-based scheduling system to notify approved subscribers (users) of upcoming network activities that may impact their service(s). The system allows users to filter notices based on key words or phrases.

3.6.5.1 NISN Corporate Freeze Policy

NISN Corporate freeze policy/process is described in the *NISN Service Document (NSD*).

3.6.6 UNITeS NISN Tier 2 Service Desk Management and Integration

The existing NISN Corporate ENMC will be the Tier 2 support that integrates with I^3P's Tier 1 Enterprise Service Desk (ESD), Section 1.3.1. The UNITeS contractor currently uses a Remedy

system to track service request and trouble tickets and has an electronic interface to a MSFC specific Tier 1 Service Desk, NASA Integrated Service Center (NISC). At some point the NISC interface will be exchanged with the I^3P Tier 1 Enterprise Service Desk (ESD).

3.7 UNITES/MOMS NISN MISSION SERVICES

UNITeS and MOMS Task Order 16 contractors are responsible for designing the infrastructure used to provide Mission services, all designs are approved by NASA. Contactor duties include the preparation of requirements analyses and a prototyping strategy for implementing the requirements, development of network architecture(s) and design, site preparation, installation, integration and testing for deployment, sustaining engineering, trouble-shooting, and preparing as-built documentation for all implemented requirements. The contractor develops network designs and operational concepts, and NASA approves the design concepts through the appropriate review channels.

In the event of incidence/problems, the contractor provides Event Report (ER) analysis and resolution, priority System Problem Report (SPR) resolution (if necessary), responds to Daily Summary Reports (DSR), and provides on-call mission availability. An example of a DSR is provided in *Example Daily Summary Report*.

NASA Mission services span multiple Centers. Wide Area Mission services are managed out of GSFC by the same personnel that manage the GSFC Local Mission services. This workforce is currently supported by both UNITeS and the MOMS contractors. With NICS the support at GSFC (both Local and Wide Area) will be consolidated into a single contract, NICS. NISN Mission services' equipment is located at over 45 locations both in the United States and Internationally. There are seven (7) major Mission Communications Centers located at various NASA sites (e.g. JSC, MSFC, KSC, GSFC's WSC, GSFC's WFF, JPL, and DFRC). The Mission Communication Center at GSFC, GSFC Communications Control (GCC), provides wide area network equipment to these sites. The other Mission Communications Center sites, which are not part of NICS, are as follows:

a. JSC's Communications Control
b. MSFC's Hubble Operations Support Center (HOSC)
c. KSC's Technical and Communications Control
d. DFRC's Telemetry and Communications Control
e. GSFC's WSC STGT, WSGT, WSC Operations Support and Scheduling
f. GSFC's WFF Communications and Range

UNITeS and MOMS coordinate with personnel, that are not part of UNITeS/MOMS (or will be part of NICS), located at the other six sites for hands on support of the NISN Mission Services equipment. Refer to *Existing Mission Service Requirements Circuits* for a listing of Mission circuits. A listing of the key Mission sites is provided in *Key and Tail Mission Sites*.

The NISN Mission services specified in this PWS are absolutely essential to the success of ALL Manned Flight and Scientific Spacecraft Missions. Failure of communications links during critical periods of flight could result in the loss of both spacecraft and in some cases the loss of human life.

The UNITeS and MOMS contractors provides for Mission sustaining engineering for all the Mission services of PWS 3.7.1 through .7. The contractor provides sustaining engineering for the implementation of Mission Service Requests for Mission work, including the installation and documentation of implemented solutions. The contractor participates in reviews (design, requirement, test, operational readiness and others) as requested. The contractor staffs this support on an 8 hours a day, 5 days a week basis, except when requested to provide mission critical or special support. Additionally the contractor provides as follows:

a. Interfaces and coordinates with communications control, as necessary and required, to provide and restore service.
b. Reports all sustaining engineering activities to the Communications Manager.
c. Documents all implementations with drawings and Engineering Changes (ECs).
d. Uses the EC format as detailed in the mission configuration management document and ISO certified processes.

For a listing of the systems and tools used in support of Mission refer to *Mission Tool Inventory.*

3.7.1 NISN UNITeS/ MOMS Mission Voice Services

Mission Voice services are currently provided using a combination of the Voice Switching System (VSS) at GSFC which provides the Mission WAN bridging functions; Carrier provided voice circuits and Center specific voice switches. MOMS provide all of the voice switch support at GSFC. At GSFC the Center voice switch is the Voice Distribution System (VDS). At JSC the Center Voice Switch is the Digital Voice System (DVS). The Mission Operations Voice Enhancement (MOVE) Project currently has a new switch installed at GSFC undergoing testing for the replacement of the VSS and VDS. NASA will transition the VSS and VDS services to the new switch during FY10, and install common MOVE switches at the majority of the Mission Centers over the next several years. Implementation of MOVE switches is not currently within the scope of the NICS contract. However, as MOVE switches are installed, NICS will be required to support the testing and transition of services from the legacy infrastructure to MOVE. NICS will not maintain the MOVE infrastructure.

Today the VSS is tied to approximately 730 carrier voice circuits and the VDS supports approximately 500 local keysets, referred to as *Mission Voice Inventory (Legacy)*. A policy decision requiring customers to pay for their own keysets is expected to reduce the number of Local Keysets at GSFC by at least 20% when the MOVE switches become operational at the end of FY-09. The current plan under MOVE is for VTO to maintain the keysets for the customers out a spares inventory and send keysets to the MOVE vendor for repair. Please refer to the

applicable document, *Mission Voice Inventory (Legacy),* for more information on Mission voice support.

Mission Voice services are primarily supported by Voice Technical Operations (VTO; e.g. MOMS Task Order 16) which operates the VSS and VDS at GSFC. The circuits are supported by UNITeS GCC. The local Mission voice switches at JSC, MSFC, KSC, JPL, GSFC's WSC, GSFC's WFF and other centers are operated by the center's local mission contractors and are not part of the NICS scope of work.

The contractor provides transmission, bridging, and switching to support a system of dedicated, mission voice circuits working in conjunction with Center switching/conferencing systems to create inter-connected voice communications loops. The voice loops interconnect the different Center voice distribution systems that support diverse missions within the Agency. The contractor provides operations, sustaining engineering, and maintenance of the Center switching/conferencing systems. In providing this service, the contractor:

a. Operates and maintains the GSFC mission switching/conferencing systems 24 hours per day, 7 days per week, at the NASA Information Category Level of "Mission (MSN)," in accordance with NPR 2810.
b. Operates the GSFC mission switching/conferencing systems and associated equipment in accordance with all applicable Security Guidelines and Operating Procedures.
c. Provides fault isolation, restoration, testing, and monitoring, including detection of circuit degradation, of all the voice circuits terminated in the GSFC mission switching/conferencing systems.
d. Establishes, maintains, and monitors voice conferences to NASA network and mission control centers and various other NASA, federal government and international partner facilities.
e. Provides on-site coverage during mission critical periods.
f. Coordinates and interfaces with government and contractor personnel regarding mission voice requirements.

3.7.2 UNITeS NISN/MOMS Mission Video Services

The contractor provides for the distribution of video signals in support of NASA programs. The particular implementation is dependent on the specific requirements of the program and may involve terrestrial or satellite transmission, with or without the utilization of digital compression and encoding techniques. Examples of current video distribution services include the following:

a. Shuttle External Tank Ice Video

Specifications: Upon launch, the Space Shuttle external tank rides piggyback to near orbital velocity, approximately 113 kilometers (70 miles) above the Earth. The now nearly empty tank separates and falls in a preplanned trajectory with the majority of it disintegrating in the atmosphere and the rest falling into the ocean. The video feed from a camera mounted on the

tank records information from the time of launch until the time of tank separation. This feed is used to determine if any ice or foam debris have potentially impacted the sensitive shuttle tiles that make up the thermal protection system. Shuttle External Tank Ice Video is supported using the same transponder as Mission TDRSS Data/Video Services. The Uplink to the Transponder is switched from KSC to WSC after Launch.

b. NASA Select
Specifications: NASA Select is a satellite television transmission network for both live and recorded programs about the entire range of NASA programs. It carries major events, such as launches, encounters with the planets, press conferences or presentations by NASA's researchers and engineers as they happen. Many of the programs are particularly applicable for educators.

c. Mission Tracking & Data Relay Satellite System (TDRSS) Data/Video Services
Specifications: The contractor maintains a one-way, multi-mode/multi-channel High Rate Data System, designed for operation over a full C-band (36 MHz) domestic communications satellite transponder. This service provides a medium for transport of a Tracking and Data Relay Satellite System (TDRSS) user's digital baseband return link when the rates are 2 Mbps or higher. The system has an upper limit for the user's data of 48 Mbps. When not used for data, the service is be used for the transmission of video information in a user's TDRSS return link from the White Sands Complex (WSC) to JSC.

The contractor provides operations, sustaining engineering and maintenance of the mission video distribution system. This includes the documentation of all operations, engineering, and maintenance, and repair activities. This includes a daily log, in accordance with Mission reporting, *UNITeS NISN Example Mission Operational Support Plan.* Key to success is the contractors' coordination with NASA customers and their associated contractor personnel regarding mission video activities. In providing this service, the contractor provides the following:

a. Normal Operations: Operate and maintain the Goddard TV Central Facility, 8:00 am to 5:00 pm, Eastern Time, Monday through Friday, at the NASA Information Category Level of "Mission (MSN)," as defined in NPR 2810.1**A**.
b. Shuttle Mission Operations: Shuttle mission support, the facility is operated 24 hours per day, 7 days per week.
c. Special Agency Programming: Record, edit, duplicate, and playback video for Agency programmatic activities such as programming in support of the Agency Administrators Meetings
d. Normal Operations: Provide switching and distribution of video feeds and transponder switching of NASA Select TV service.
e. Mission Operations: Provide on-site coverage during mission critical periods.

3.7.3 UNITES NISN/MOMS Mission Routed Data Services

The contractor provides the hardware, software, routing, management, and operations necessary to support NASA's Mission routed data requirements. The contractor supports Internet Protocol (IP) as the Agency's standard for routed data services and legacy non-IP protocols until they are phased out.

Two service performance categories for Mission routed data services have been defined:

a. Real-time Critical
b. Mission Critical

Performance requirements for these services are specified in the NISN Document 001-001, *NISN Services Document*. Customer request for services that do not fall within these requirements are considered under Mission Dedicated Data and Customer Services, 3.7.5

Mission Routed Data Services are currently provisioned on three separate segments of the IP Operational Network (IONet) and on a number of project specific networks such as EBNet, IDEA and ISS FEPR networks. The three segments of IONet are as follows:

a. Closed IONet
b. Restricted IONet
c. Open IONet

These segments are differentiated by security policies and posture. Closed IONet is the most restrictive segment and supports a large number of real time critical command and telemetry requirements. It also supports the UDP multicast flows associated with legacy encapsulated 4800 bit block requirements.

For a briefing on IONET service classifications refer to the applicable document entitled *IONET Briefing.*

The contractor supports several intra-domains routing protocols on the Mission Routed Data Service including the following:

a. Static, Routing Information Protocol (RIP)
b. Enhanced Interior Gateway Routing Protocol (EIGRP)
c. Open Shortest Path First (OSPF)

Additionally inter-domain routing protocols such as Border Gateway Protocol (BGP) are supported. The contractor coordinates with customers to select a protocol consistent with both the customer's requirement and the common network architecture.

The NISN Goddard Communications Control (GCC) manages all of the networks segments that support Mission Routed Data Services. They currently manage 730 network devices (Routers, Switches, Hubs, FDDI Concentrators) at forty-five (45) sites that are distributed to many buildings at GSFC, KSC, JSC, MSFC, WSC, JPL, DFRC, WFF, CONUS and International Partner Locations.

3.7.4 UNITeS NISN/MOMS MISSION Integration Services

The Mission Integration Service consists of two primary components:

a. Mission Communications Manager
b. Communications Manager

3.7.4.1 Mission Communications Manager

The contractor supports Mission Integration Services by assigning a Mission Communication Manager to each mission or project using an expendable launch vehicle. The Mission Communication Manager is responsible for working with specific missions/projects before and during the mission/project to develop and implement an Operational Support Plan for that particular Mission or Project.

a. Prior to the mission/project the Mission Communications Manager coordinates extensively with each Shuttle Mission or Project using an Expendable Launch Vehicle to understand their communications and support requirements. This is documented through operational readiness reviews. Examples of an ORR for both a mission and a project are found in applicable documents, *Example Mission ORR* and *Example Project ORR* in applicable documents.
b. The Mission Communication Manager creates an Operational Support plan for approval by the mission/project. An examples of an Operation Support Plan for both a Mission and a project are found in applicable document, *UNITeS NISN Example Mission Operational Support Plan, UNITeS NISN Example Project Operational Support Plan.*
c. The Mission Communications Manager sits on console during critical coverage periods and provides the dedicated Communications Manager functions for that specific Mission.
d. The Mission Communication Manager must be knowledgeable of all NISN MISSION Services and be able to direct the operations staff on how to resolve incidents or problems. Therefore the contractor provides the following:
    1) Annual Training and Certification for each Mission operations support function for NASA approval.
    2) Annual certification training to include: written tests in the areas of Mission-critical operations, on-the-job training, and on-the-job skill assessment.
    3) Examples of which are *Mission Communications Control Operator Training,* and *UNITeS Mission Training Requirements.*

3.7.4.2 Communications Manager

The contractor provides a Communications Manager who manages the day-to-day operations of all the Mission Services. The Communications Manager currently supports the UNITeS NISN Wide Area Network and the GSFC MOMS Local Mission Network from GSFC. There are similar, communications manager type people at other centers that are not part of UNITeS NISN/MOMS, and therefore are not part of NICS. The UNITeS contractor Communications Manager provides the following:

a. Staffs the on-console position of Shift Communications Manager, 24 hours a day, 7 days a week.
b. Reports problems and obtain status.
c. Interfaces with missions and projects to receive requests for service repairs and other functions required of the entities in the NOMC.
d. Furnishes information to missions and projects concerning service outages and troubleshooting that pertain to them.
e. Responsible for coordinating all functional areas to provide Mission Services.
f. Responsible for prioritizing problem troubleshooting and restoration activities.
g. Responsible for problem escalation.
h. Responsible for coordinating all work during mission freeze periods.
i. Responsible for logging and reporting outages and activities.
j. Prepares and send Mission Outage Notifications (MONS) to the appropriate distribution for all outages meeting the established criteria.
k. Prepares and send a Daily Summary Report (DSR) to the defined distribution.
e. The Shift Communication Manager must be knowledgeable of all NISN MISSION Services and be able to direct the operations staff on how to resolve incidents or problems. Therefore the contractor provides the following:
    1) Annual Training and Certification for each Mission operations support function for NASA approval.
    2) Annual certification training to include: written tests in the areas of Mission-critical operations, on-the-job training, and on-the-job skill assessment.
    3) Examples of which are *Mission Communications Control Operator Training,* and *UNITeS Mission Training Requirements.*

3.7.5 UNITeS NISN/MOMS Mission Dedicated Data and Custom Services

Although NASA encourages the use of routed data services, if a customers requirements do not fit into the routed data service they are provided with dedicated data and customer services. Based on NASA approval, the contractor provides customers with full-time, dedicated bandwidth between two or more discrete locations, due to performance and/or security considerations, or to support unique data transfer protocols not otherwise supported by the routed data network. The contractor documents and provides rationale for use of dedicated services. The contractor uses GSA contracts for the procurement of the bandwidth.
Examples of Mission Custom Networks are as follows:

a) ISS Downlink Enhancement Architecture (IDEA)
Specifications: ISS Downlink Enhancement Architecture (IDEA) currently dedicated OC-3s from WSC to JSC and to MSFC with Juniper M-5 Routers. This interface supports ISS K-Band Requirements. This service is being migrated to Layer 2 Ethernet Services on the NISN/NASCOM Mission Backbone as part of the Obsolescence Driven Avionics Replacement (ODAR) Project.

b) Solar Dynamics Observatory (SDO)
Specifications: SDO is designed to help understand the Sun's influence on Earth and Near-Earth space by studying the solar atmosphere on small scales of space and time and in many wavelengths simultaneously. SDO is Solar Dynamics Observatory. They are using a new ground station located at White Sands Complex. Their network is built out with Layer 2 Ethernet Services on the NISN/NASCOM Mission Backbone and Juniper routers.

c) Front End Processor (FEPR)
Specifications: ISS Front End Processor Replacement (FEPR) Dedicated Network supporting ISS S-Band Command and Telemetry. This interface uses Layer 2 Ethernet Services on the NISN/NASCOM Mission Backbone and Juniper 6350 routers and is designed for real time Critical Requirements.

d) Meteorological Information Data Distribution System (MIDDS)
Specifications: MIDDS is the principle meteorological data display system for both SMG and the 45th Weather Squadron (45 WS), and an auxiliary display system for the National Weather Service in Melbourne, Florida (NWS MLB).All data collected in the Kennedy Space Center (KSC) / Cape Canaveral Air Station (CCAS) area are transmitted to SMG through MIDDS at the Range Operations Control Center (ROCC).

3.7.5.1 Mission Software Development

A key task the contractor performs for this service is the development and maintenance of software for systems whose requirements cannot be met using Commercial Off-the-Shelf (COTS) software. This includes the Small Conversion Devices and the Tracking Data System. Current software development is focused on two systems, Small Conversion Devices and Tracking Data System. The contractor provides the following software engineering support:

a. Engineering Software Releases: The contractor performs requirements analysis, system design, coding, configuration management, and testing for software releases. The contractor holds software design reviews prior to new version releases.
b. Maintaining Related Software: The contractor performs application modifications to support network requirements and modifications to correct software issues. The contractor supports the maintenance of several tools (e.g. debuggers, traffic generators, and traffic capture software) that provide system test and network

capabilities, diagnostic and fault isolations capabilities, and network traffic data collections capabilities.

c. Distributing Upgrades: The contractor supports the distribution of operating systems upgrades, security patches/fixes, kernel upgrades, custom kernel upgrades, and custom serial drivers.
d. Mission information management and network management tools sustainment, maintenance and release development/testing. A list of the tools supported is found in *Mission Composite Tool Inventory* in applicable documents.

3.7.6 UNITeS NISN/MOMS Center-Specific Mission Services

UNITeS does not provide for any Center-Specific Mission Services. MOMS Task Order 16 includes the Mission LAN that supports GSFC and as such is included in the activities of Mission Routed Data.

3.7.7 UNITeS Mission IT Security Services

The contractor supports the engineering of security systems within the Mission Network to include, but not limited to: Patchlink server, and host scanning system. The contractor works in conjunction with the Mission services engineering functions above in verifying and specifying the appropriate security controls and design that meet Federal, Agency, NISN, and Mission security requirements in accordance with NPR 2810. The categories of network traffic captured, stored, and analyzed must be approved by the Mission NSO. The contractor performs as follows:

a. Collects and assess security requirements against network data flow requirements and define network firewall implementation. The contractor also supports incident investigation and IT security incidents/emergency response in coordination with the Mission Network Security Officer (Mission NSO).
b. Performs quarterly vulnerability scanning consistent with the current network scanning architecture and approach and report scanning findings and metrics quarterly.
c. Supports and maintains the government's secure web server to distribute vulnerability reports.
d. Establishes an intrusion detection architecture and approach and deploys accordingly.
e. Perform network traffic analysis based on monitoring from Mission It Security Operations Support.
f. Reports all identified intrusions to the Mission NSO and reports intrusion detection findings monthly to the Mission NSO.
g. Establishes a security incident response team to support the Mission NSO. With coordination from the NASA monitor, the contractors serves as a network and host computer security-engineering group providing consultation and intrusion evaluation services to the Mission community.

3.7.8 UNITeS NISN/MOMS Mission Configuration Management and Documentation

Configuration Management and Documentation ensures that all work in the Mission Support Areas is properly coordinated under Engineering Changes (ECs) and Release Requests and that all UNITeS/MOMS organizations have current versions of supporting documentation to work with. In close coordination with the UNITeS/MOMS organizations the contractor records and maintains the following:

a. Source/Destination Code Handbook
b. Network diagrams/drawings
c. Standard operating procedures and guidelines
d. IT Security Plans and related documentation
e. Ensures that all software configurations are made in sets of three accompanied by a delivery letter. One set is maintained in the NOMC, another is secured in the Security Control Center safe and a third is secured in the Security Control Center safe within the Emergency Control Center.

3.8 UNITES NISN/MOMS MISSION MANAGEMENT AND OPERATIONS

Mission Management and Operations responsibilities are currently split between the UNITeS Contract and the GSFC's Mission Operations Management Support (MOMS) Task Order 16. Both the UNITeS and MOMS Task Order 16 work will be consolidated into NICS. The various tools used for NISN/MOMS MISSION Management and Operations can be found in *UNITeS-MOMS Mission Tools Inventory* in applicable documents.

3.8.1 UNITeS NISN/MOMS Communications Control

Communications Control performs the day-to-day operations and troubleshooting of the Mission communications. The Communications Control function is at each NASA that supports mission or projects project using an expendable launch vehicle. The Communications Control function for the UNITeS NISN Wide Area Mission Service and GSFC MOMS Local Services map to Goddard Communications Control, Voice Technical Operations and Goddard TV in today's environment and will consolidate into NICS.

a. Communications Control is responsible for day-to-day management and operations of Mission Services. The contractor performs as follows:
    1) Staffs on-console positions, 24 hours a day, 7 days a week, during day-to-day, mission-critical, and special support unless otherwise noted.
    2) Reports all anomalies and the results of all subsequent restorations to the Shift Communications Manager (Communications Manager).
    3) Maintains a Mission Network Operations Log to log all operations, testing, and restoration activities.
b. Communications Control manages and operates the Mission Routed Data WAN and LANs and performs fault isolation and troubleshooting. The contractor performs as follows:

1) Monitors frame/cell switched and routed networks using Government furnished Network Management System (NMS) and workstations.
2) Monitors all network problem isolation and resolutions.
3) Compiles traffic statistics for network optimization and engineering.
4) Provides updates for configuration management for all infrastructure components.
5) Coordinates maintenance issues and work with maintenance providers to maintain, repair, and upgrade network equipment.
6) Responsible for scheduling the testing all new configurations and/or configuration changes for the IONet.
7) Operates IPNOC Network Management System (NMS) using Commercial Off-The-Shelf (COTS) tools.
8) Monitors the IONet firewall and any related firewall tools.
9) Monitors IONet Domain Name Servers (DNS).

c. Communications Control manages/monitors the IONet small conversion devices and performs fault isolation and troubleshooting. The contractor performs the following:
    1) Manages, operates and troubleshoots conversion devices used in the network as gateways between the legacy 4800 bit block and the Internet Protocol (IP).
    2) Manages and operates conversion devices for operational and testing support of missions and projects, according to approved requirements and mission briefings.
    3) Reconfigures conversion devices to maintain and support missions and projects as necessary and required.
    4) Provides troubleshooting, restoration for conversion devices in order to maintain support for missions and projects.
    5) Generates Secure Gateway Requests associated with conversion devices.
    6) Assigns network data routing codes (source/destination, logical port addresses and fixed multicast addresses), as necessary and required
    7) Provides updates to the Source/Destination Code Handbook containing network data routing codes and maintain the security level of the handbook according to the applicable NASCOM Security Guidelines and Operating Procedures.

d. Communications Control manages and operates the Mission Voice Switches at the Centers and performs fault isolation and troubleshooting. The contractor performs the following:
    1) Manages, operates, configures, and troubleshoots mission voice systems used to provide mission voice service, in the form of digital switching and conferencing, for mission and projects.
    2) Establishes, maintains, and monitors voice conferences, according to approved requirements and mission briefings.
    3) Provides fault isolation, restoration, testing, and monitoring of all voice circuits terminated in the systems.

e. Communications Control manages the interface to the Commercial Carriers that provide Mission Critical Services and performs fault isolation and troubleshooting. The contractor provides:
    1) Staffs and maintains the control capability that is operational 24 hours per day 7 days per week at the NASA Information Category Level of "Mission (MSN)," as defined in NPR 2810.1A.
    2) Provides configuration of high speed, wideband and video transport systems to meet specific mission requirements.
f. Communications Control manages and operates the Mission Video Services and performs fault isolation and troubleshooting. The contractor performs the following:
    1) Provides operations of the Goddard Space Flight Center's video distribution system to support missions, projects and organizations.
    2) Provides and distributes timing references for control centers.
    3) Operates the Goddard Space Flight Center TV Central Facility, 8 hours a day, 5 days a week, except when necessary and required to provide on-site coverage during mission critical or special support periods.
    4) Performs recording, editing, dubbing, and playback of video for mission and Goddard Space Flight Center programmatic activities.
    5) Provides switching and distribution of video feeds throughout Goddard Space Flight Center.
    6) Provides transponder switching of the NASA Select TV service.

3.8.1.1 Operations Centers

For Mission operations both NISN UNITeS Mission Wide Area and GSFC MOMS Local Area Mission Operations support is provided out of the Network Operations and Management Center (NOMC) located at GSFC. Many of the NASA Centers will also have components of Mission Operations Support. In order to meet availability and restoration requirements for Mission Services, the Mission Operations contactor at each center coordinate with and support the NISN UNITeS/MOMS Mission operations contractors.

3.8.1.2 Mission Operations Clearances

The contractor ensures that each employee assigned to a Mission Operations Support function is eligible to work in a National Resources Protection Physically Secured Zone. Although only the IT security personnel of PWS 3.7.7 and 3.8.4 require DoD secret clearances, it has been helpful that engineers and operations personnel also hold a DoD Secret. At this time approximately sixty (60) people hold a DoD Secret clearance that supports Mission Services.

3.8.2 UNITeS NISN/MOMS Installation and Maintenance

The UNITeS and MOMS contractors provides for the maintenance of Mission infrastructure that is located at each NASA Center with Mission Services. The contractor participates in reviews (design, requirement, test, operational readiness and others) as requested. The contractor staffs these services on an 8 hours a day, 5 days a week basis, except when requested to provide mission critical or special support. The contractor provides the following:

a. Performs physical installation of equipment and cables in support of Mission Services as follows:
    1) Installs systems and equipment racks as required to implement requirements
    2) Provides and maintains the cable plant and associated systems required to provide mission video, mission data, TV, and precision timing references.
    3) Maintains approved documentation of the cable plant to track the connections and available fibers in the cable plant.
b. Performs preventative maintenance on equipment supporting Mission Services.
c. Performs Line Replicable Unit (LRU) replacement on equipment supporting Mission Services.
d. Supports the GSFC Modular Repair Lab (MRL) that repairs LRU modules for a number of otherwise non maintainable services. For additional data related to the LRUs that GSFC Modular Repair Facility repairs, refer to *Modular Repair Lab Capabilities* in applicable documents.
e. Performs System Administrator functions for Mission Systems by ensure that all IT Security controls are implemented in full compliance with NASA directives.
f. Logs all maintenance and repair activities.

3.8.3 UNITeS NISN/MOMS Network Scheduling

The contractor provides scheduling and coordination to optimize the operation of all NISN Mission WAN and GSFC Mission LAN entities. The work period is normally performed 7:00 am to 7:00 pm, Central Time, Monday through Friday. The contractor performs the following:

a. Provides scheduling of satellite transponders, systems and circuit releases used in the network.
b. Distributes communication alert messages to network users and common carriers notifying them of mission critical support periods.
c. Issues preliminary and final service advisory messages as necessary.
d. Provides on-site coverage during mission critical periods, as defined by the COTR.
e. Maintains a daily log of all network-scheduling activities.
f. Coordinates and interface with the government and other contractors in accordance with government guidance.
g. Provides an e-mail-based activities scheduling system, which notifies approved users of user-impacting activities at least 10 calendar days prior to conducting the activity.
h. Provides a feedback mechanism for customers to request cancellation or rescheduling of activities.
i. Provides an electronic mail-based outage notification system to inform approved users of major service outages.
j. Provides for Activity and Outage reports archival and makes this available via the web to approved users. The contractor coordinates who has access to this archive system and archived information with the COTR-designated personnel and ensures no unauthorized users gain access.

k. Adheres to NASA mission freeze policies which disallow network changes during mission-critical periods, follow the NASA freeze exemption request and waiver process, and coordinate requests for exemptions to network freezes.

3.8.3.1 Mission Freezes

Two primary approaches that are used to satisfy the critical nature of these communications requirements are provisioning redundant paths (e.g. by design) that are diverse from each other and implementing Mission Freezes during critical periods.

Mission Freezes is a primary factor affecting work in Mission Management and Operations. As a result of these freezes the Mission Services infrastructure were frozen approximately 41% of the total time available in FY-08.

The Mission Services infrastructure was frozen approximately 45% of the core hours (7 am to 7 pm Eastern Mon through Fri) during the same time period. Work on the Mission Services Infrastructure is normally performed during these core hours because Missions are supported 24 hours per day and 7 days per week. Working during core hours maximizes the support available for troubleshooting if there are any problems associated with the work.

In order to meet Mission requirements a Freeze Exemption Request (FER) process has been established to allow work to occur during Mission Freeze Periods after careful scrutiny of the risks associated with that work on the Mission Service infrastructure is frozen for. In FY-08 215 FERs were processed. Approximately 48% of the FERs were written to allow work by external organizations with the Facilities Management Division at GSFC (FMD) accounting for approximately 35%. Refer to the applicable document, *FY-08 Freeze and FER Analysis* for more detailed information of freezes and FERs information.

3.8.4 UNITeS NISN/MOMS Mission IT Security Operations Support

The MISSION IT Security Operations support consists of two primary functions as follows:

a. Mission IT Security
b. Security Control Center

3.8.4.1 Mission IT Security Operations

The contractor administers the security operational systems to include, but not limited to, Patchlink server and the host scanning system as follows:

a. Coordinates with the Mission IT Security Service engineering and planning activities providing the day to day reports as required.
b. Supports incident investigation and IT security incidents/emergency response in coordination with the Mission Network Security Officer (Mission NSO).

c. Operates and manages the Mission intrusion detection infrastructure, and perform network traffic monitoring.
d. Supports Mission IT Security Service engineering with traffic monitoring results relating to all identified intrusions.
e. Performs IONet Security Audits

3.8.4.2 Mission Security Control Center

Special facility requirements are required for Mission operations, as such the MOMS contractor provides the cleared personnel to control this facility. The contractor provides the following:

a. Provides support to the NASCOM programmatic security operations, configuration management, and Communications Security (COMSEC) programs and all NASCOM operation facilities, where appropriate.
b. Staffs the NASCOM Security Control Center, 8 hours a day, 5 days a week during normal support. The contractor provides 24x7supports at the request of the Code 731 Mission Operations Manager when necessary to cover critical coverage periods.
c. Provides physical security control, electronics systems control, and security configuration management of all NASCOM operations facilities, according to the applicable NASCOM Security Guidelines and Operating Procedures.
d. Reports all security anomalies, or breaches, to the Communications Manager and the NASCOM System Security Officer (SSO).
e. Interface and coordinate with all areas of the NOMC, including the IPNOC, as necessary and required, to provide security services.
f. Logs all security operations. The appropriateness of the contents of the log is coordinated with the SSO.
g. Provides security support to the SSO, the COMSEC Manager, and the Crypto Security Officer for NASCOM's programmatic security operations and security configuration management

3.8.5 UNITeS NISN/MOMS Mission Facilities Management

In support of NISN/MOMS the contractor is responsible for the GSFC facilities general cleaning and coordination of facility upkeep with GSFC facilities.

3.9 UNITES NISN CUSTOMER RELATIONSHIP MANAGEMENT

NISN uses Project/Program Service Level Agreements (PSLAs) to document customer requirements, associated service implementations, and pricing information. NISN maintains PSLAs with each NASA Center, and with Projects and Missions who require NISN services. NISN Service Managers (NSM), civil service staff under the NISN Project, are responsible for designated customers and their requirements but are assisted by UNITeS in all aspects of Customer Relationship Management. UNITeS supports the development, maintenance, review, and approval of PSLAs, and provides support to the annual PSLA validation process. UNITeS maintains a PSLA application and database, which contains the requirements baseline and

changes to requirements, implementations, and pricing information. Examples of PLSA's are provided as follows:

a) *NISN Fairmont IVV PSLA Agreement*
b) *NISN Fairmont IVV PSLA Supporting Data*

NISN, along with support from UNITeS, also maintains the *NISN Services Document (NSD)*, which describes NISN's approved service offerings, service levels and policies and processes for obtaining these services.

3.9.1 UNITeS NISN Customer Service Representatives (CSRs)

UNITeS provides Customer Service Representatives (CSRs) who are assigned to each NASA center, JPL, MAF and NASA Headquarters. These CSRs are responsible for interfacing with customers at their respective sites regarding requirements, service requests, service implementations, service updates, user training, and performance reporting to customers. These individuals also interface with non-NISN, civil servant representatives established at each NASA Center and for specific programs. NISN Center/Program Representatives are senior NASA civil servant personnel who are able to commit their organization in areas such as the communications networks budget, requirements for service, and policy. Specific functions of a NISN Center/Program Representatives are:

a. Gathering and verifying network requirements
b. Coordinating requirements with NISN Customer Interface Group
c. Initiating requests for studies or cost estimates to the NISN organization
d. Receiving and facilitating the distribution of NISN information
e. Participating in center/program requirements reviews
f. Interfacing with the NISN Team
g. Coordinating local installation activities in support of NISN services
h. Representing Center/Program at NISN Customer Forums
i. Facilitating validation of NISN billing information for services
j. Coordinating funding issues
k. Identifying issues and areas of concern
l. Providing contract evaluation input.

The current listing of NISN Service Managers, Customer Service Representatives (CSR) and NISN Center/Program representatives may be found at the following web site: http://nisn.msfc.nasa.gov/ContactPages/CustomerInterfaces.html.

NASA has established Center Customer Commitment Managers (CCCMs) to be responsible for the process that results in one or more commitments being made between the Space Communications and Navigation (SCaN) program, NISN and a space project. These commitments define the total set of services that are to be provided by SCaN to the project. NISN supports these CCCMs and their contractors by providing expertise for NISN requirements

and services. CCCM assignments may be found at the following web site: http://nisn.msfc.nasa.gov/ContactPages/CustomerInterfaces.html.

On an annual basis, NISN hosts a Customers' Forum. UNITeS provides coordination and contracting for hotel guest rooms and meeting space, coordination and implementation of audio/visual and communications services (phones, wireless network, projectors, sound system); customer notification and registration; agenda development and presentations; and support for breakout meetings with customers. UNITeS also provides similar support for a pre-Forum planning meetings held either at MSFC or GSFC a few months before each Forum. UNITeS customer service participates in customer site visits with each NASA facility.

The tools that the contractor uses to support this function are found in *NISN Corporate Network Tools*.

3.10 UNITES NISN SERVICE MANAGEMENT

3.10.1 UNITeS NISN Facilities Engineering

The UNITeS contractor works with center/CIEF designated personnel on NISN gateway installation or other NISN CIEF or points of presence to ensure compliance with applicable center/CIEF specifications, regulations.

3.10.2 UNITeS NISN Service Delivery Support Software

UNITeS provides procurement of COTS tools, in-house development of, maintenance for and upgrades/refresh of NISN Service Support applications. The UNITeS contractors provide system administration, software integration, and software development for a host of tools that support all aspects of NISN services. The tools, *UNITeS NISN Integrated Service Delivery Tools,* include a variety of application types, operating systems, languages and require a variety of software skills.

3.10.2.1 NISN Service Requests

UNITeS maintains the NISN Service Request System (NSRS) which are used by Customer Service Representatives (CSR) to submit service requests on behalf of customers. NSRS is used by various UNITeS functional organizations, CSR, Engineering, Configuration Management, Financial Management etc., to process and track service requests to completion. In FY08, NISN CSRs initiated 586 new NSRs with 72 of these NSRs being canceled sometime during the fiscal year. Details regarding the NSRS customer-facing process may be found on the NISN website at: http://nisn.msfc.nasa.gov/DocumentPages/Processes.html.

3.10.3 UNITeS NISN Configuration Management

The NISN customer services are documented in the *NISN Services Document*, located at http://www.nisn.gov . The contractor, working closely with the NASA technical monitors, keeps this key customer document up to date and published.

Under NICS, the contractor will coordinate with the I^3P to maintain the appropriate service categories in the NASA *Enterprise Service Directory*.

Additionally the contractor currently provides and will be expected to provide under NICS, customer facing NISN Service Level Agreements (SLAs), Organization Level Agreements (OLA's) (e.g. between NASA's infrastructure) and Underpinning Contract (UC) that the contractor may have with vendors. The following documentation is provided as samples:

a. *NISN Services Document (note: This includes NISN SLAs)*
b. *NASA Enterprise Service Directory*
c. *SOC-NISN SLA*

3.11 UNITES NISN STRATEGY GENERATION

The NASA IT environment is a constantly changing environment with innovations continuously introduced. NASA must constantly investigate and evaluate new information technologies and initiatives that offer the possibility of improving service delivery, reducing costs, and changing how the Agency does business today and in the future. As an organization, NASA encourages initiatives and the pilot projects that assess the applicability and business value of next-generation emerging technologies. Innovative technologies that offer promise for improving the manner in which information services are delivered today must then be integrated into the existing NASA architecture with minimal disruption to our customer base. Based on NASA's unique mission, it must constantly be at the forefront of technology, exploring those technological opportunities that offer the most promise.

NISN, with UNITeS contractor support, collaborates with both the NASA OCIO/I^3P and MSFC on business/technical planning and governance. This includes various aspects of business and technical activities to support the analysis of service, infrastructure and process for technology insertion and overall improvements. These activities typically culminate in a business case that has to be approved through the OCIO/I^3P governance prior to becoming an approved project. Examples of types of deliverables associated with this activity are as follows:

a. *Strategic Institutional Investment Proposal for Augmenting the Agency's Corporate Network Infrastructure (Redacted) (e.g. WANX)*
b. *NISN AIM EA Data Call*
c. *MSFC Five-Year Information Technology Plan*

The activities of strategic planning will be led by the I^3P and coordinated with NICS, ACES, EAST, WEST and center CIO specific governance entities. The NICS contractor will be required to work with both I^3P and Center-specific governance entities as applicable, to collaborate on NICS areas that are related to the strategic planning services, infrastructure, and process of NICS. Ultimately all strategic planning for NICS must be approved by the OCIO/I^3P. The data below is provided as background and historical data to describe the various strategic planning

activities that the NICS contractor will have to support with MSFC and/or other specific centers and OCIO/I^3P.

3.11.1 UNITeS NISN Strategic Planning

The UNITeS contractor currently provides subject matter expertise in support of NISN IT strategic planning functions. This effort results in a yearly strategic planning report and the development of business cases for consideration by I^3P governance decisions.

3.11.2 UNITeS NISN Support to the Enterprise Architecture

The UNITeS NISN contractors supports by research, evaluating, and recommending best practices in enterprise architecture as it relates to networks; reviews, assesses, and recommends changes in the direction of the Agency enterprise architecture; develops composite enterprise architecture artifacts that represent the as-is and future states of the Centers' enterprise architecture; develops and maintains an integrated enterprise architecture document repository; analyzes, documents, and reports the composition of the Centers' application and infrastructure portfolio; develops and documents NISN segment architectures; and conducts enterprise architecture progress reviews of major IT program segments. NICS Strategy Generation, PWS Section 3.11, will conform to the guidelines provided in compliance with OCIO/I^3P.

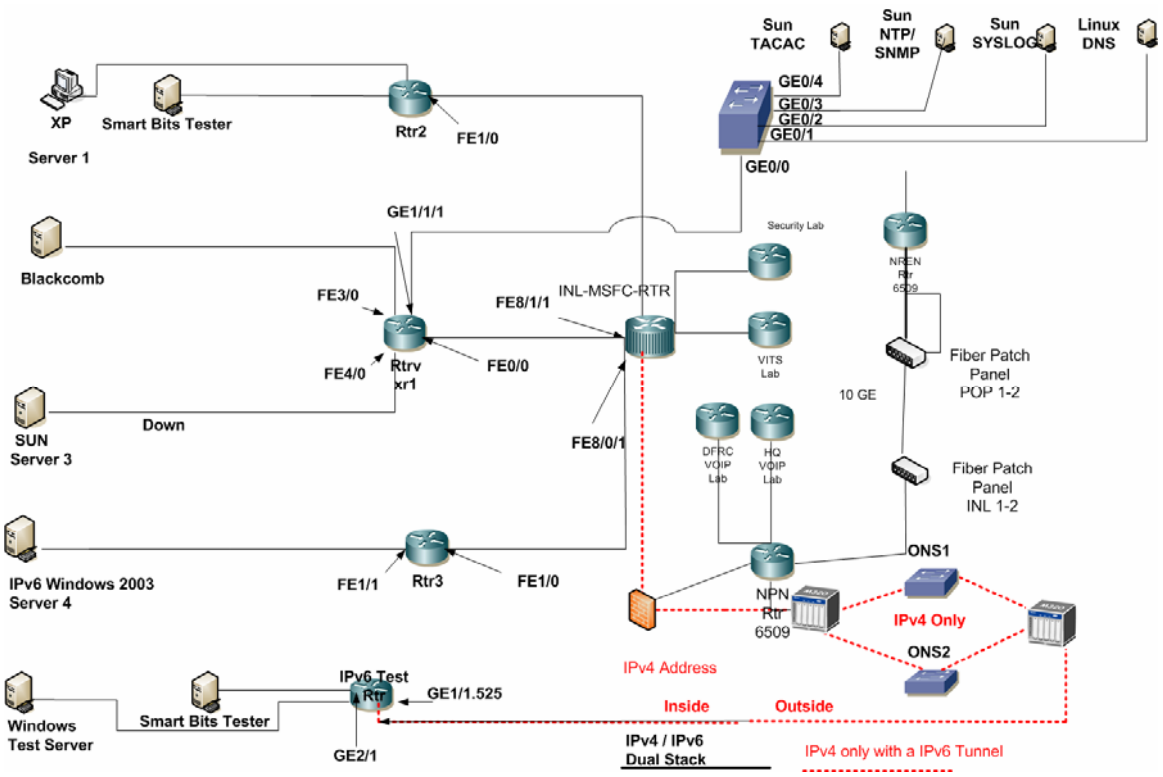
3.11.3 UNITeS NISN Corporate Network Capacity Planning

NISN performs capacity analysis and planning activities to ensure the network architecture continues to support growing customer requirements in a timely manner. Each NSR generates a modification to the capacity management database, which represents consolidated requirements for each NASA Center, MAF, JPL, and Headquarters. These consolidated requirements are used to initiate architecture, design and/or procurement activities to accommodate validated requirements.

3.11.4 UNITeS NISN Network Modeling

NASA continues to foster the transition of application and protocols to the NASA operational network (NISN). To be able to support the emerging demands of the NISN customers, NISN continually develops engineering expertise in emerging systems and technologies. To that end, NISN has a lab to evaluate technologies and perform modeling and simulations, the NISN Operations System Laboratories (NOSL). The NOSL, maintained by UNITeS, is located at Marshall Space Flight Center (MSFC) and consists of a routed and optical layered network laboratory supporting both operations and system testing requirements. This limited support for the NOSL is approximately 1 WYE engineer and 1 WYE technician. The NSRs and specific projects dictate the need/usage of the lab. The figure below illustrates the NOSL local network configuration.

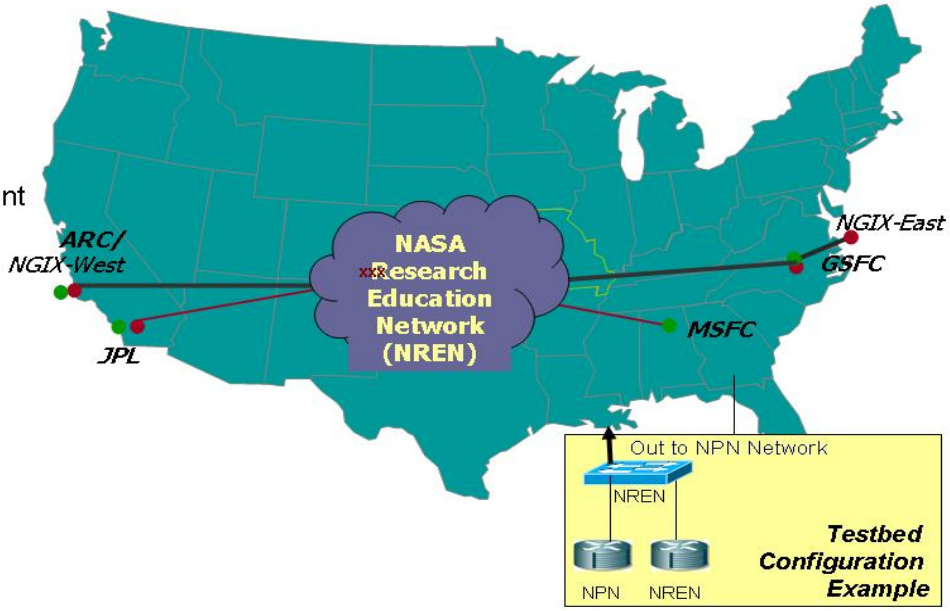
NISN Operation System Laboratory (NOSL) Configuration



The NOSL staff represents NASA at conferences and working groups to development an understanding of the trends and changes in evolving network technologies, such as the Joint Engineering Team (JET), North American Network Operator Group (NANOG), Internet II, IPv6 Summits. It maintains an engineering proficiency in leading technologies to develop an understanding of the implementation of communication systems. The group helps to transition knowledge and prototypes into the operational NISN, and collaborates with engineers, laboratories, and other Federal Networks with like interests. The figure below illustrates the connectivity into the NASA Research Education Network (NREN).

NISN Operations System Laboratory (NOSL) Enterprise Connectivity

- Network Hardware
  - Juniper
  - Cisco
  - APC
- Test Equipment
  - Spirent
  - Anue
  - Victoria
  - SUN
  - Microsoft
- Network Management Systems
  - Netscout
  - Concord
  - Sun
- Carriers
  - National Lambda Rail



The table below is a sample of were the NOSL was used to by NSRs or projects to evaluate the applicability of the technology to NISN:

Project	Key Tasks	Protocols	Network or Video/Voice Resources	Systems
NASA Collaborative Initiative (NCI)	Develop and test H.264 (MPEG-4) Integrate AES module into the VITS lab testing and prototyping MCU. Evaluate AES. Smartcard integration into the VITS system.	H.264 Advance Encryption System (AES)	Multipoint Control Unit (MCU) Controllers Digital Devices Smartcard	Web Server MS Outlook
Internet Protocol version 6 (IPv6)	Develop and evaluate Internet IPv4 and IPV6 tunneling mechanisms. Implement multicasting across the NPN for evaluation and testing. Begin phases of IPV6 network security testing. Complete IPV6 DNS testing.	IPv6 OSPF BGP	Routers Switches	Web Server Ftp Server DNS Server Network Management Systems
Voice over Internet Protocol (VoIP)	Finalize integration of the wireless system into the test bed. Evaluate latest version of the Cisco Express Call and Unity manager. Prototype a soft phone solution allowing VoIP installation onto personnel laptops.	Session Initiation Protocol (SIP)	Soft Phones Phones Voice Routers Voice Switches	Call Managers Unified Messaging Systems
Wide Area Network Replacement (WANR)	Evaluate network technology imports to determine operational impact.	MPLS BGP Lambda	Routers Switches	eHealth Opnet

3.12 UNITES NISN IT SECURITY SERVICES

NASA utilizes a proactive and re-active Agency-wide coordinated team effort to ensure that all IT Security components are secure and have a fast reacting team to deal with vulnerabilities or incidents that might occur. This includes notification, incident response, database centralized collections, tracking and analysis, including forensics of IT Security activities. NISN is a member of this agency wide team.

3.12.1 UNITeS NISN /Incident Response

NISN provides network anomaly sensors at all NASA Field Centers and HQ. Anomalies are sent to the SOC for processing

3.12.2 UNITeS NISN IT Security Perimeter

Each center has specific IT security perimeter controls typically using smartcard access to buildings and rooms. Additionally the UNITeS NISN gateways have specific perimeter controls in support of the NIST classification of ‘medium’ these are all documented in the NISN 2810 Security Plan subsections on IT security controls.

3.12.3 UNITeS NISN Security Operations

The contractor establishes and maintains contact with internal and external technical working groups consisting of IT and IT Security professional associations, NASA Field Centers, and vendor systems experts to assist in accomplishing its mission. This includes supporting Computer Emergency Response capabilities from other government and industry organizations, both national and international. The contractor also supports NASA by attending various meetings and working groups to discuss issues and concerns regarding activities and functions in all IT Security areas.

Activities are provided for IT technical support at NASA Field Centers and in coordination with external incident handling entities to support IT Security Vulnerability Notification and Incident Response roles and responsibilities. These activities include: working in a collaborative partnership with NASA Centers and Agency-wide projects; working with NASA senior management to develop and test prototypes of IT Security tools, techniques, or training that may be planned for all NASA Field Centers; and working and coordinating with external entities such as the Federal Computer Incident Response Capability (FedCIRC).

The Firewall team maintains, configures, and operates firewalls for Agency-wide services. The MSFC Agency Public Network Firewall protects servers and systems to which MSFC external users require access. These services are placed on a network, which is separate from MSFC's networks.

Support is provided in the administrative coordination and technical support for all daily operations and planned upgrades with the SOC. Support is provided to handle vulnerability notifications and incident detection, emergency coordination and recovery, and ongoing tracking and analysis responsibilities for the benefit of the NASA Agency (including the federal and contractor staffs).

SOC has established and maintains contact with internal and external technical working groups consisting of IT and IT Security professional associations, NASA Field Centers, and vendor systems experts to assist in accomplishing its mission. SOC specifically supports Computer Emergency Response capabilities from government and industry, both national and international at the discretion of the SOC. SOC attends regularly held working group meetings to discuss evolving issues and concerns regarding the activities and functions of SOC operations and to formulate recommendations for improving operations and/or reducing any potential risk exposures for NASA.

SOC supports NASA Field Centers with coordinating external incident handling entities in support of their roles and responsibilities, which includes working in a collaborative partnership with agency-wide projects like the NISN on agency-wide 24x7 vulnerability notification and incident coordination initiatives; working with NASA senior management to test prototypes of IT Security tools, techniques, or training that may be planned for a broader roll-out to all NASA

Field Centers; and working and coordinating with external entities like Federal Computer Incident Response Capability (FedCIRC).

3.12.3.1 NISN Clearances Needed for Security Operations

The contractor employees must be screened in accordance with NPR 1600.1, *NASA Security Program Procedural Requirements*. For IT security, personnel require a minimum NACI with ability to get a higher clearance. IT Security personnel must have a certifications in Intrusion Detection or experience equivalent. Forensic and Systems Administrators must have a certification from a credible source or equivalent training.

3.13 UNITES NISN GSA CONTRACT INTEGRATION

For WAN services, NASA purchases telecommunications services (e.g. switched voice, dedicated data, conferencing services) via Government-Wide Acquisition Contracts (GWACs) such as GSA's Federal Technology Service (FTS) and Networx contracts, when those contracts meet NASA's requirements or can be modified to meet NASA's requirements. UNITeS supports NASA in procuring these services via the GSA FTS and Networx contracts.

3.13.1 GSA CONTRACT INTEGRATION

The UNITeS contractor provides integration and support functions in support of NASA's purchase of GSA FTS2001 and Networx services. GSA has recently awarded the Networx contracts which will replace the legacy FTS2001 contracts, which are expiring. NASA is currently in the process of performing fair opportunity consideration to select Networx contractors and is transitioning services from the old FTS2001 contracts to the new Networx contracts.. For NASA's use of FTS2001/Networx services, in addition to those services provided by FTS/Networx, the UNITeS contractor:

a. Matches NASA requirements to GSA contract solutions and identifies any exceptions where the GSA contract solutions do not meet NASA requirements.
b. Generates technical designs that include the use of GSA contractor-provided services.
c. Supports the NASA FTS2001 and Networx CO(s) and COTR(s) in performing fair opportunity, including preparing and tracking requests for quotations, performing market research, and evaluating GSA contractor quotations to determine whether the quotations are technically acceptable and represent fair and reasonable pricing.
d. Supports the NASA FTS2001 and Networx CO(s), the COTR(s), and GSA in initiating, coordinating, and reviewing quotes for GSA contract modifications and NASA master agreement/delivery order modifications.
e. Ensures that all UNITeS contractor personnel are properly trained regarding Designated Agency Representative (DAR) responsibilities and that all personnel comply with Federal and NASA procurement regulations relative to the use of GSA telecommunications contracts (for example, performing fair opportunity in accordance with FAR Part 16.505).
f. As NASA DARs, initiates, prepares, submits, and tracks service orders on the GSA contracts and escalates any issues related to processing of these orders.

g. Initiates, submits, and tracks requests for new accounts, deletion of accounts, and changes to accounts on FTS2001 and Networx contractor business systems and for FTS2001 and Networx services.
h. Coordinates GSA FTS2001 and Networx service orders and service order issues with the UNITeS contractor's internal organizations (for example, engineering, operations, business functions) and with NASA.
i. Supports the NASA FTS2001 and Networx CO(s) and COTR(s) in performing acceptance testing of new services and performs ongoing monitoring of services delivered by the GSA contractors to ensure that the delivered services are in accordance with the requirements specified in the GSA's FTS2001 and Networx master contracts, NASA's master agreement/delivery orders, and individual service orders.
j. Monitors GSA contractor(s) performance relative to requirements, and reports results to FTS2001 and NASA Networx CO(s) and COTR(s).
k. Coordinates network management and operations functions with GSA contractor(s), including but not limited to, sharing of network monitoring and problem resolution information and processes, sharing of trouble ticketing information, and maintenance and exercise of escalation processes.
l. Conducts GSA contractor billing analysis, to include:
    1. Maintenance of NASA's Agency Hierarchy Code (AHC) in accordance with NASA's requirements to report usage and billing to multiple accounts.
    2. Ensuring that all service orders and associated invoices contain the correct AHC.
    3. Review and reporting of all GSA Contractor bills to ensure that the Contractor(s) are billing in accordance with the requirements specified in the GSA's master contracts, NASA's master agreement/delivery orders, and individual service orders.
    4. Initiates, documents, files, tracks, reports, reconciles, and escalates billing disputes with GSA Contractor(s) and ensures that billing credits are applied to the correct NASA account..
    5. Identifies and reports to NASA any instances of fraud or abuse of GSA Contractor services.
    6. Creates, maintains, and distributes GSA and FTS2001 and Networx contractor billing reports and data to report costs by consumer (e.g., center, program/project, user, account).
m. Reviews new/changed/deleted GSA contractor service offerings to determine the impact to NASA users.
n. Coordinates project management of activities related to transition of any GSA Contractor services to new or different contract vehicles or service offerings.

UNITeS initiates approximately 19 Mission service orders per month and 16 Corporate service orders per month to the FTS/Networx contractors; these service orders require integration with UNITeS-provided systems, issuance and tracking of GSA FTS2001/Networx service orders, and coordination with service locations during implementation

As of January 2009, NASA/NISN was approximately 10% complete in all of its transitions from the FTS2001 contracts to the Networx contracts.

NASA/NISN has chosen centralized billing for all FTS2001 and most Networx services, allowing for better visibility, assessment, and management of the overall NASA costs for these services. GSA receives the FTS2001 and Networx Contractor cost detail in flat file format from the various FTS2001 and Networx contractors. The billing information is received by UNITeS and NASA up to five weeks after the end of the month being billed. GSA posts the cost data to a web-based reporting tool, which is accessed by UNITeS. The GSA billing information is a summary of the monthly costs that are billed to NASA.

UNITeS also receives flat file data from each FTS2001 and Networx Contractor and merges the GSA and FTS2001 Contractor data using agency hierarchy codes and FTS2001 and Networx bill payer identification as reference points. The billing data is merged using Excel and is separated by service. The billing data is further allocated to the NASA centers and projects including contractor sites. The data is summarized and forwarded to a list of authorized personnel.

The summary information related to NISN's effort to perform fair opportunity consideration to select Networx Contractors is provided at the following website: http://nisn.nasa.gov/networx.

It should be noted that the performance specifications included in NASA's Networx requests for quotation and in the GSA Networx master contracts are specific to the telecommunications services being procured by NASA on Networx and should not be confused with the performance specifications applied to NICS.

To better understand the GSA FTS2001 and Networx support provided by UNITeS the following table depicts the summary UNITeS GSA interactions for FY08:

GSA Contract Integration Work Load Indicators						
FY07	**Type**	**Mission**	**Approximate Mission $$**	**FY07**	**Mission Support**	**Approximate Corporate $$**
Adds	Private Line circuits	61	$ 270,000	Adds	47	$ 145,000
Adds	Switched Voice	0	$ -	Adds	37	$ 6,059
Disconnects	Private Line circuits	118	$ (163,000)	Disconnects	43	$ (87,000)
Cost Quotes	Circuits	87	$ -	Cost Quotes	59	$ -
Totals		266	$ 104,000	Total	186	$ 64,000
FY08				**FY08**		
Adds	Private Line circuits	62	$ 315,000	Adds	62	$ 315,000
Adds	Switched Voice	0	$ -	Adds	0	$ -
Disconnects	Private Line circuits	88	$ (278,000)	Disconnects	88	$ (278,000)
Cost Quotes	Circuits	80	$ -	Cost Quotes	80	$ -

3.13.1.1 Additional GSA Workload Actions

The UNITeS contractor provides for the following in support of GSA contract integration:

a. Monthly billing data validation, allocation and reconciliation
b. Monthly billing summary reporting and distribution
c. Ad hoc data analysis (for example, traffic analysis, billing queries)
d. Ongoing analysis of billing data analysis to identify and report errors and omissions
e. Continuous follow-up with vendors to track, report, and coordinate service delivery due dates and technical specifications

3.13.1.2 Purchased Telecommunications Services

For telecommunications services that are not available on GSA contracts or when requested or approved by NASA, UNITeS purchases telecommunications services circuits via subcontracts. Examples of these services include domestic circuits that are not offered on GSA FTS2001, satellite services, and transatlantic and in-country circuits support Russian services. In these cases, UNITeS procures, monitors, coordinates, and pays for all aspects of these circuit deliveries.

3.14 UNITES NISN/MOMS WORK LOAD INDICATORS

3.14.1 UNITeS NISN Corporate Work Load Indicators

3.14.1.1 Contract Direct Hours

The document *UNITeS Direct Labor Hours* (UNITeS Direct Labor Hours.doc) depicts direct labor hours for UNITeS PWS 3 NISN for calendar year 2007 and 2008.

3.14.1.2 Corporate Network Trouble Tickets

In support of NISN, UNITeS processes corporate Network Trouble Tickets the following documents provides insight to this work load:

a. *UNITeS NISN Work Load Indicators August 2008*
b. *UNITeS NISN Trouble Ticket Summary*

3.14.1.3 Corporate Purchase Orders

In support of NISN, UNITeS processed the following number and dollar value of purchase orders in FY07/08:

Number of Purchase Orders	VALUE ($)	YEAR
644	19,000,000	2007
619	17,000,000	2008

3.14.1.4 Corporate Network Vendor Maintenance

In support of NISN, UNITeS processed the vendor maintenance as delineated in *UNITeS VENDOR MAINTENANCE IN SUPPORT OF NISN FY08.*

3.14.1.5 NISN User Training

Several of the NISN services have components that are delivered directly to the end user. Examples of these include video teleconferencing, voice teleconferencing, and calling cards. Service operations manuals are developed and made available to customers for self-training or for one-on-one training as requested. As each new service is added, a training plan for the customer is developed if needed. Training materials are reviewed yearly to ensure accurate service information.

User guides for NISN applications and services are also made available to customers and NISN personnel. Training materials for these systems are made available to internal team members and customer representatives so that training of individuals can take place as new accounts are established.

Publicly available, existing training materials can be found at the following link: http://nisn.msfc.nasa.gov/DocumentPages/UserGuides.html.

3.14.2 UNITeS NISN/MOMS Mission Work Load Indicators

3.14.2.1 Mission Direct Hours

The document *UNITeS Direct Labor Hours* (UNITeS Direct Labor Hours.doc) depicts direct labor hours for UNITeS PWS 3 NISN for calendar year 2007 and 2008.

3.14.2.2 Mission Trouble Tickets

In support of NISN, UNITeS/MOMS processed Mission Network Trouble Tickets as provided in *NISN UNITeS/MOMS Mission Trouble Tickets FY08.*

3.14.2.3 Mission Network Vendor Maintenance

In support of NISN, UNITeS processed the vendor maintenance as delineated in *UNITeS VENDOR MAINTENANCE IN SUPPORT OF NISN FY08.*

In support of NISN, NASCOM UNITeS/MOMS processed the vendor maintenance as delineated in *Mission Maintenance.*

3.14.3 NISN UNITeS Mission and Corporate Network Service Request

The UNITeS Mission and Corporate Network Service Request (NSRs) collected during FY08 are documented *in NISN Mission and Corporate FY08 Network Service Requests (NSR's).*

3.15 APPLICABLE DOCUMENTS

The following is a listing of applicable documents for background and historical section 3.0.

Located at the I^{3}P Technical Library http://i3p-acq.ksc.nasa.gov

a. NASA Enterprise Service Directory
b. NPR 2810.1A, Security of Information Technology

Located at the MSFC Directives:
https://repository.msfc.nasa.gov/directives/

a. MPR 8715.1, *Marshall Safety, Health, and Environmental (SHE) Program*

Located at the NISN information:
http://www.nisn.nasa.gov/DocumentPages/Documents.html

a. NISN 001-001, *NISN Services Document*
b. NISN 3000-4323, *NISN Service Request System (NSRS) Process*

Located at NICS, Other Documents, B&H Applicable Documents
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. *Agencywide ViIP Initiative*, (Agencywide ViIP Initiative.doc)
b. *ENMC Network Management System (NMS) Refresh CCB Presentation,* (ENMC-NMS Refresh-CCB-021909.ppt)

c. *Collaboration Services- ViTS Rooms,* (Collaboration Services- ViTS Room.xls)
d. *Example 1: ViIP NSR,* (Example1-VIIP NSR.pdf)
e. *Example 2: ViIP NSR*, (Example2-VIIP NSR.pdf)
f. *Example Daily Summary Report* (Example Daily Summary Report.dc.rtf)
g. *Example Mission ORR,* (Example Mission ORR.ppt)
h. *Example Project ORR,* (Example Project ORR.ppt)
i. *Example: ViIP Audio*, (Example-VIIP Audio.ppt)
j. *Example: Custom Full Service ViIP*, (Example-Custom Full Service ViTS.ppt)
k. *Example: Custom ViIP Custom Multimedia*, (Example-VIIP Custom Multimedia.ppt)
l. *Example: ViIP Roll-About*, (VIIP Roll-About.ppt)
m. *Existing Mission Service Requirements Circuits,* (Existing Mission Service Requirements Circuits.doc)
n. *FY-08 Freeze and FER Analysis,* (FY-08 Freeze and FER Analysis.xls)
o. *IONET Briefing,* (ionet_briefing2008.ppt)
p. *Key and Tail Mission Sites,* (Key and Tail Mission Sites.doc)
q. *Mission Composite Tool Inventory, (Composite Tool Inventory3-10-09.xls)*
r. *Mission Maintenance,* (NASCOM_EOL_LIST_20090305_v2.xls)
s. *Mission Tool Inventory,* (Mission Tool Inventory.xls)
t. *Mission Voice Inventory (Legacy),* (Mission Voice Inventory (Legacy).xls)
u. *Mission Communications Control Operator Training* (Mission Communications Control Operator Training.doc)
v. *UNITeS Mission Training Requirements (*UNITeS Mission Training Requirements.*xls)*
w. *Modular Repair Lab Capabilities,* (Modular Repair Lab Capabilities.doc)
x. MSFC CIO IS-01-008*, Information Technology Risk Management*, (IS01-OWI-008.pdf)
y. *MSFC Five-Year Information Technology Plan*, (Five_Year_IT_Plan_2006.pdf)
z. *NASA Teleconferencing Services and VIIP Network Overview* , (ViIP Overview Rev2.doc)
aa. *Network Management Case Study*, (NM_Case_Study_final.doc)
bb. *Networx: Amendment 3 CLIN Grouping 3, Tail Circuits,* (GSA Networx Tail Circuits (Amendment 3).xls)
cc. *Networx Performance Work Statement J-2 Backbone Group 2 (BG-2), Regional Circuits*, (Networx ATTACHMENT J-2 Amendment 1.doc)
dd. *Networx: Performance Work Statement J-1 Backbone Group 1 (BG-1), Core Circuits*, (Networx Core Backbone Circuits SOW.doc)
ee. *NISN AIM EA Data Call,* (NISN AIM EA Data Call.xls)
ff. *NISN Corporate Gateways Addresses*, (NISN Corporate Gateway Addresses.doc)
gg. *NISN Corporate Network Tools*, (UNITeS NISN Corporate Network Tools.xls)
hh. *NISN Fairmont IVV PSLA Agreement*, (NISN Fairmont IVV PSLA Agreement.pdf)
ii. *NISN Fairmont IVV PSLA Supporting Data*, (NISN Fairmont IVV PSLA Supporting Data.xls)

jj. *NISN Gateway and CSR Facilities*, (NISN Gateway and CSR Facilities.xls)
kk. *NISN Mission and Corporate FY08 Network Service Requests (NSR's)*, (NISN Mission and Corporate FY08 Network Service Requests .xls)
ll. *NISN Service Request (NSR) Processing Procedure*, (4519 RevF (NSR Processing).doc)
mm. *NISN UNITeS/MOMS Mission Trouble Tickets FY08,* (NISN UNITeS-MOMS Mission Trouble Tickets FY08.xls)
nn. *NRS User Guide*, (0013_NRS_User_Guide.doc)
oo. *NTC Brochure*, (NTC Brochure_DRAFT.pdf)
pp. *OMB Memorandum M-08-27, Guidance for Trusted Internet Connection (TIC) Compliance,* (m08-27.pdf)
qq. *Draft_TIC_Conceptual Architecture (Draft_TIC_Conceptual Architecture092008.pdf)*
rr. *SOC-NISN SLA,* (SOC-NISN-SLA-2009-02-23.doc)
ss. *Strategic Institutional Investment Proposal for Augmenting the Agency's Corporate Network Infrastructure (Redacted),* (Strategic Institutional Investment (SII) proposal for WANX_redacted.doc)
tt. *UNITeS Direct Labor Hours*, (UNITeS Direct Labor Hours.doc)
uu. *UNITeS NISN CONUS Circuits*, (UNITeS NISN CONUS Circuits other than Networx.xls)
vv. *UNITeS NISN Example Mission Operational Support Plan,* (UNITeS NISN Mission Operational Support Plan.xls)
ww. *UNITeS NISN Example Project Operational Support Plan, (*UNITeS NISN Project Operational Support Plan.xls)
xx. *UNITeS NISN Integrated Service Delivery Tools,* (UNITeS NISN Integrated Service Delivery Tools.xls)
yy. *UNITeS NISN Trouble Ticket Summary,* (UNITeS NISN Trouble Ticket FY07 through fy08.xls)
zz. *UNITeS NISN Work Load Indicators August 2008,* (UNITeS Work Load Indicators.ppt)
aaa. *UNITeS VENDOR MAINTENANCE IN SUPPORT OF NISN FY08*, (NISN Vendor MaintFY08.xls)
bbb. *UNITeS-MOMS Mission Tools Inventory,* (UNITeS-MOMS Mission Tools Inventory.xls)
ccc. *ViIP Certification for VCS Room Packages*, (ViIP Certification for VCS Room Packages.doc)
ddd. *ViIP Configuration Document*, (VIIP Configuration Document.xls)
eee. *ViIP Overview Presentation*, (ViIP.ppt)
fff. *ViTS ISDN Directory*, (ViTS ISDN DIRECTORY.xls)
ggg. *ViTS over IP Services (ViIP) Migration Plan White Paper*, (ViIP Migration Plan Rev5.doc)
hhh. *Vots and ViIP Statistics*, (VIIP Statistics - 2008.xls)
iii. *Vots Directory*, (VoTs Directory.xls)

jjj. *VoTs User Guide*, (0012_VoTs_User_Guide.doc)
kkk. *VRA User Guide*, (0014_VRA_User_Guide.doc)
lll. *WANX Preliminary Project Plan, (WANX-005_(Project Management Plan) Preliminary.doc)*

The following documents are available on CD-ROM and may be requested in writing on company letterhead from:

Jeff Jackson
OFC: PS31, Procurement Office
NASA, George C. Marshall Space Flight Center
MSFC, AL 35812
256-544-8935
jeffery.s.jackson@nasa.gov

a. *IPAM System Design Document,* (IPAM-023(System Design Document).doc)

4 CENTER AND ASSOCIATED COMPONENT FACILITY SERVICES

4.1 AMES RESEARCH CENTER (ARC)

Ames Research Center (ARC) is located in Northern California on Moffett Field in the heart of Silicon Valley. ARC supports approximately 4500 total users, dispersed between approximately 65 individual buildings.

4.1.1 Property/Inventory

The ARC network supports approximately 750 network devices, excluding all client nodes. Property may be stored onsite, see Facilities description (PWS 4.1.7) for the amount of onsite storage used under the existing contracts.

4.1.2 Shipping/Receiving/Inspection

The contractor will use ARC provided shipping and receiving services.

4.1.3 Vehicles Necessary To Support Center Work

The Ames CIO organization has about five (5) vehicles available for checkout.

4.1.4 Physical Security

The contractor will work with Ames Protective Services for keys and physical access to facilities.

4.1.5 Emergency Management

The ARC Emergency Operations System provides wireless and voice services in the event of disaster that renders the standard ARC network unusable. The system includes a satellite system, a wireless LAN controller and network infrastructure.

4.1.6 Safety

The contractor must adhere to the Ames Health and Safety Manual, including participation in confined space training and asbestos awareness training.

4.1.7 Facilities

ACITS2 personnel occupy onsite space at ARC in five (5) buildings not including the space allocated for telecommunications shown in the table below as technical space. The following is a listing by type of space.

Type of Space	SQUARE FOOTAGE
Office Space	3,500
Technical Space	15,000

Storage	1,500
Lab	1,000
Conference Room	700
Miscellaneous	

This space allocation is located primarily in the buildings N233, N263, N158, N229, N240 and telecommunications "facilities" in all other buildings.

The majority of office space is located in N233.

The personnel to support the NS3 Contract are located at ARC in Building 258. A description of the space requirements follows below:

Type of Space	SQUARE FOOTAGE
Office Space	80
Technical Space	5 rooms x 2 RU + 1 room x 8 RU
Storage	Included in Office Space
Lab	N/A
Conference Room	N/A
Miscellaneous	Included in Office Space

4.1.8 Network Services

Network services include IPAM, RAS, NTP, and Guest Network services.

4.1.8.1 IPAM

Ames has been migrated to the Agency IPAM in 2008. There are three IPAM systems at ARC, providing both DNS and DHCP services.

4.1.8.2 RAS

Remote Access Services for ARC clients include client-based VPNs terminated on 4 Cisco 3080 VPN concentrators for IPSec based VPNs. In addition a Juniper Neoteris SSL VPN is provided. Authentication for these services is provided using a RADIUS front-end, which accesses either a users active directory credentials, or an ACE platform using SecurID tokens.

4.1.8.3 NTP

Ames provides ntp.nasa.gov as a resource to the general public.

4.1.8.4 Guest Network

The Ames wireless system provides two wireless networks: ARC-WLAN (NASA), used by ARC employees for access to ARCLAN-OPEN, and ARC-WLAN-GUEST (NASA-guest), used by guests and visiting employees for limited web, mail and VPN access. ARC-WLAN-GUEST uses a Captive Portal system with a self-registration form that allows guests to request accounts for themselves with the actual credentials delivered in a secure fashion to an Ames employee sponsor, who must have an email account on the NOMAD system.

All 275 Aruba access points provide connectivity for both networks simultaneously, and are distributed across 61 buildings within Moffett Field. The three (3) GoNetworks access point provide access to ARC-WLAN-GUEST only, and provide connectivity to buildings M583A and B for NASA Exchange Lodge guests.

The Local Controllers serve as endpoints - all of an AP's traffic is tunneled through its controller, which also performs Air Monitoring, Wireless IDS and other functions. The Local Controllers report to the Master Controller to allow for client mobility, configuration management and reporting. All Master and Local controllers are redundant.

The ARC-WLAN is a “client only” network which has default deny inbound access. Outbound access is unlimited for TCP/UDP ports under 10000. Access to ARCLAN Private is provided by Client to Network Cisco VPN solution or the Juniper SSL-CPN solution with two-factor authentication.

Guest users are treated like the Internet users for access to any ARCLAN resources accessible from the general internet. A VLAN is maintained for the guest network with limited direct access to ARC private IT resources. Outbound access is limited to established critical protocols (e.g. http(s), pop(-ssl), smtp(-ssl), imap(s), SSH, VPN). The guest network is “Client only” networks with default deny inbound. Printers are allowed on this network with static DHCP addresses for the convenience of printing services for guest users at select locations.

4.1.9 Data Services

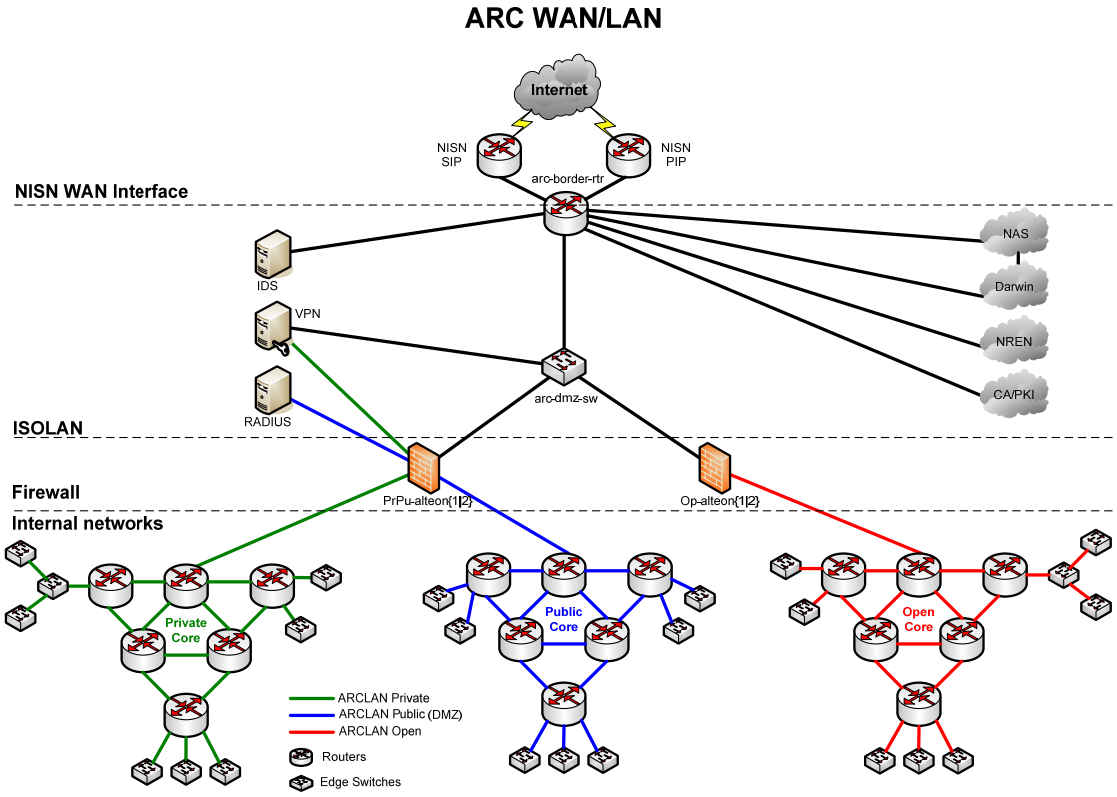
4.1.9.1 High Level LAN Description

The Ames Research Center Local Area Network (ARCLAN) consists of a standard Core/Distribution/Access Layer architecture. There are three separate physical networks, each representing a separate security domain. The core and distribution layers are fully routed using OSPF. All Core to Core links utilize Gigabit EtherChannel. All distribution layer devices are dual homed utilizing Gigabit to separate cores. The core layer consists of Foundry BigIron 8000’s. The distribution layer is largely Foundry 4802’s with some Cisco 4000 series devices for specific applications and projects. Our data center distribution layer is currently supported by a dedicated BigIron 8000, which is being upgraded to dual 6509 chassis. Our access layer is comprised of largely Cisco closet switches, which are usually single-homed at 100 Mbps to the

distribution layer over copper. One core per security domain is dual gigabit connected to a redundant firewall system, which in turn is connected to a Cisco 6509 DMZ switch which in turn is connected using GigEtherChannel to a Cisco 6506 Border Router. The border router is connected to SIP and PIP utilizing one Gigabit Link each. The border architecture is currently in transition to a new architecture that will eliminate the DMZ switch and redeploy it as a redundant border router.

a. Ames Center LAN (Intranet)

The ARCLAN Private Network is largely comprised of client desktop workstations, with some "Infrastructure Server components", including active directory and file sharing resources. For the most part, this is a client only network, in that only connections initiated from inside private are allowed. There are exceptions for a few protocols, including managing inbound SSH sessions, and mail connections through a center mail relay system.



b. Ames Private Network (ARCLAN Private)

The Ames Private Network is part of the Ames Intranet. This network hosts all client nodes and access is restricted to connection states being initiated from inside the network.

This is typically a desktop or client network and is the most populated network. This LAN has limited inbound access allowed through the firewalls (registered SSH servers, bi-directional VPN, etc.) and default deny in-bound. From this network you can access most ARCLAN public servers for administration purposes. Most applications up through IP TCP/UDP port 10000 allowed outbound to the Internet, and all applications that use ports above 10000 are managed. ARCLAN Private is considered trusted NASA IP Space.

c. Ames Public Network (ARCLAN Public)

The Ames Public network is an isolated network available across the Ames campus. This network hosts systems that are accessible from the Internet or agency only resources and off. These devices include Remote Access devices, FTP servers, web servers, mail servers, and many other applications. No client desktops are allowed on this LAN. It is the least populated network and has the highest security level allowed with limited inbound protocols allowed through the firewalls. Most applications up through TCP/UDP port 10000 are allowed outbound to the Internet, and all applications that use ports above 10000 are managed. ARCLAN Public is considered trusted NASA IP space.

d. Ames Open Network (ARCLAN Open)

The Ames Open Network represents a "catch all" for all the client and server nodes whose connectivity or security requirements cannot be met by either the Ames Public or Private network. This is also the network where point to point connections to teaming partners are permitted. There are several highly purposed project resources with non-standard security, management, or bandwidth requirements that exist on this network.

There is a heavy reliance on host-based firewalls, project firewalls, and tight system administration to manage security risk associated with open access to these resources. Access to public network resources limited to essential infrastructure components (AD, DNS, NTP, etc.). Otherwise, ARCLAN Open is treated like the Internet. Connectivity to Private from Open is provided by Client to Network Cisco VPN or Juniper SSL-VPN solutions with two-factor authentication. Outbound traffic from ARCLAN Open is mostly unfiltered, except for some established "bad" protocols.

4.1.9.2 Wireless Networks

The system provides two wireless networks: ARC-WLAN (NASA), used by ARC employees for access to ARCLAN-OPEN, and ARC-WLAN-GUEST (NASA-guest), used by guests and visiting employees for limited web, mail and VPN access. ARC-WLAN uses WPA2/AES and WPA/TKIP for authentication against Active Directory.

All 275 Aruba AP's provide connectivity for both networks simultaneously, and are distributed across 61 buildings within Moffett Field. The 86 Aruba AM's provide dedicated Air Monitoring for RF analysis and intrusion detection.

The Local Controllers serve as endpoints - all of an AP's traffic is tunneled through its controller, which also performs Air Monitoring, Wireless IDS and other functions. The Local Controllers report to the Master Controller to allow for client mobility, configuration management and reporting. All Master and Local controllers are redundant.

Access to the ARCLAN Private is provided by Client to Network Cisco VPN solution or the Juniper SSL-CPN solution with two-factor authentication.

4.1.9.3 Network Security

The Ames Intranet is further segmented by utilizing IT Security managed internal firewalls. All Ames firewalls are centrally managed and monitored by IT Security and Network Engineering. Currently there are four intranet firewall systems that provide security between the three (3) Center LANs at Moffett Field.

4.1.9.4 Network Operations

Network management services are hardware and software applications that provide monitoring and management services for the network infrastructure. The hardware currently implemented is Dell Hardware. Network management software implemented includes:

a. inMon: Network Traffic Management Tool
b. ipMonitor: Network Monitoring and Availability
c. Spectrum: Proactive Monitoring, Trending, Network Fault Management System

Network management displays are available via web browser and are also displayed in the Ames Network Operations Center. The Ames Network Operations Center is located in building N233 and provides displays for network management/monitoring hardware. The NOC supports seating for approximately six personnel.

4.1.9.5 Network Processes

Under the current operational model, the contractor is pre-authorized to fulfill standard requests such as moves, adds and changes. When the contractor is implementing a non-standard request, such as changing a router configuration or adding/removing hardware, the change must be elevated to the civil servant network manager.

4.1.9.6 Network Lab

ARC has a small lab with a limited set or hardware that is representative of models used in the ARCLAN. This lab is mainly used for configuration change testing.

4.1.9.7 Hardware Description

The core layer consists of Foundry BigIron 8000's. The distribution layer is largely Foundry 4802's with some Cisco 4000 series devices for specific applications and projects. Our data center distribution layer is currently supported by a dedicated BigIron 8000, which is being upgraded to dual 6509 chassis. Our access layer is comprised of largely Cisco closet switches, which are usually single-homed at 100 Mbps to the distribution layer over copper

4.1.9.8 Hardware Refresh

Ames has an equipment replacement goal of five years, largely dependent upon funding, to keep equipment on the LAN current and serviceable by the vendor.

4.1.10 Collaboration Services

One main Center ViTS facility is funded under the current NISN model, and some other customer funded rooms are NISN supported.

4.1.11 Customer Relationship Management

Information to be provided by Center, data not yet not yet available.

4.1.12 IT Security

Ames has a single IT security plan for all services that will be provided by NICS.

4.1.13 Cable Plant Services

4.1.13.1 Optical Fiber

Core: 288-strands single-mode, terminated in fiber hub Buildings N229, N233 & N240 in structured wiring closets, in compliance with industry-standard guidelines, on patch panels.

Spoke: 24-strands single-mode/12-strands multimode (50 um), deployed as hub/spoke configuration, terminated at fiber hub buildings N229, N233 & N240 and over sixty far-end buildings in structured wiring closets, in compliance with industry-standard guidelines, on patch panels.

Legacy: Various strand counts (six to twenty-four), both singlemode and multimode (50 um), terminated at over eighty far-end buildings in structured wiring closets, in compliance with industry-standard guidelines, on patch panels.

4.1.13.2 Twisted Pair Copper Cabling

Category 5E (tested to 1000Mbps or below) installed in over 15% of buildings). Wiring is terminated in structured wiring closets, in compliance with industry-standard guidelines, on patch panels.

Category 5 (tested to 100Mbps or below) installed in over 60% of buildings. Wiring is terminated in structured wiring closets, in compliance with industry-standard guidelines, on patch panels.

The remaining buildings are wired with a mix of UTP and termination types, most incapable of operating above 10Mbps.

4.1.14 Emergency Warning Systems (RESERVED)

4.1.15 Public Address Systems

Several buildings including the ARCJET facility have legacy to new public address systems installed. These systems are supported on an "as needed" basis and are not on a general maintenance cycle.

4.1.16 Radio Services

4.1.16.1 Centerwide Trunking Radio Infrastructure

This task supports the maintenance and operation of the Center-wide T-Radio system and all associated land mobile radios and systems specially integrated to utilize the radio trunking system for communications purposes. This support includes the maintenance, repair, reprogramming services, operational, administrative and customer support on Ames' M/A-Com EDACS digital T-Radio repeater system, and up to 600 associated portable, mobile and base station end user radios.

The T-Radio system consists of:

a. Seven 406-420 MHz radio repeater transceivers and Turbo GE Trunking Cards (GETCs)
b. Primary and backup transmit and receive antenna systems
c. Site Interface Module (SIM) and other directly associated radio repeater station equipment
d. Communications System Director (CSD) system software, a tool that is utilized to configure the trunking radio system (limited to upkeep of the radio Electronic ID (EID) database and use of the performance monitoring tools). All other functions available through use of the CSD are limited to the ARC civil servant managers.

End user equipment will be modified and repaired when needed. All system documentation, pre-maintenance records, repair and programming logs, the T-Radio user matrix database, CSD user/radio/system configuration database, and the tasks Standard Operating Procedures manual are kept relevant in accordance with any changes to the system warranting change.

Government Furnished Equipment (GFE) and vehicles used in support of the project, such as the RF communications test sets, and 50-ohm coax connecting tools, are made available to the contractor to support their daily operations and maintenance duties. If required, Ames RF Spectrum Management program test equipment, such as spectrum analyzers, field strength meters, frequency counters, antenna analyzers, etc., can be checked-out from the Center RF Spectrum Manager. This equipment is not to be re-loaned out by the staff, and is to be immediately returned to Spectrum Manager when they are no longer required.

4.1.16.2 T-Radio System Technical Requirements

a. T-Radio system hub located in N254, Room 109:
   (1) Inspect all station equipment cabinets and coaxial lines within the cabinets for any tampering or damage weekly. Alert Task Requester if any problems are discovered
   (2) Check cabinet temperatures and door filters weekly. Correct any problems observed, report to Task Requester, and alert the Ames External Interface (EI) personnel if further corrections need to be supported.
   (3) Take weekly measurements of the Standing Wave Ratio (SWR) for all the repeaters coaxial lines. Alert Task Requester if any of the system's seven repeaters report an SWR of greater than 1:7.
   (4) Vacuum inside of all cabinets and clean all door filters monthly.
   (5) Perform a pre-maintenance check, and if applicable, system realignment on T-Radio repeaters, Turbo GETC' transmitter combiner, receiver multi-coupler/amplifier, and antenna systems quarterly. Results of each pre-maintenance check are reported to the Task Requester in writing.
b. T-Radio narrowband conversion:
   (1) On an as funded by customer basis, process user radio equipment that qualifies for narrowband upgrading to the manufacturer (M/A-Com) for conversion.
   (2) On an as funded by customer basis, procure, and configure narrowband replacement mobile/portable radio equipment for end users.
c. Security Dispatch Console System located in N241, Room 105A (assuming customer funding):
   (1) Inspect the radio dispatch console operator modules, console switch rack equipment, and all system-associated punch down blocks and cabling for any deterioration, or other damage or tampering to the equipment weekly. Alert Task Requester immediately if any problems are discovered.
   (2) Vacuum inside of the console operator module cabinets and around the console switch rack monthly. Alert Task Requester if any problems are discovered.

(3) Provide and document upgrades and modifications to the system as required.

d. Fire Station Public Address ring down system located in N241 and M580 (assuming customer funding):
   (1) Inspect the Fire Station Public address ring down system and associated switch rack, dedicated copper landlines, VHF transceivers and antenna systems through designated telephone and PA system interface demarcations for any deterioration, damage, and tampering weekly. Immediately alert Task Requester if any problems are discovered.

e. Air Traffic Control Tower VHF-UFH air to ground dedicated radio landline link located in the M158 exterior communications close next to room 128 (assuming customer funding):
   (1) Inspect the system's relay equipment and dedicated landlines at both building M158 and N241 for any deterioration, damage, and tampering weekly. Immediately alert Task Requester if any problems are discovered.

Permanent or temporary corrections are to be implemented when responding to all valid trouble calls on the trunking radio repeater system, security dispatch console system, fire station ring down system, ATC VHF/UHF radio link, or any security, fire, or safety mobile radio system. Temporary corrections put in place by contractor staff in an effort to make the system operable in a timely fashion must be approved by the Task Requestor prior to contractor staff departing the scene. All temporary corrections must be followed-up with a permanent solution in a timely manner, at which time the trouble ticket may be closed.

4.1.17 Telephone Services

Ames primarily utilizes a Nortel Digital phone system for standard phone service. Transition to VOIP is currently in the evaluation phase and pilots are being conducted.

4.1.17.1 Number of Trunks

ARC supports 13 trunks (PRIs/T1s). Eight (8) PRIs are used for local, Direct-In-Dial (DID) and Direct-Out-Dial (DOD); Four (4) PRIs are for long-distance, FTS carriers (Verizon, MCI, Sprint); and One (1) PRI is for the Defense Switched Network (DSN).

4.1.17.2 Call Processing

All calls in and out of the center are handled by a Nortel SL-100 SuperNode SE switch installed in 1988, and upgraded to SuperNode SE06 in 2004. Approximately 4000 analog and digital phone sets are supported.

4.1.17.3 Voice Mail Services

ARC has a Rolm/Siemens PhoneMail system installed in 1989 located physically on Center; Six (6) nodes currently servicing 4700 plus subscribers.

4.1.17.4 E911 Services

ARC has three (3), outbound Centralized Automatic Message Accounting (CAMA) trunks and three (3), inbound 9-1-1 lines. A Telident Station Translation System (STS) interfaces the Ames PBX with the PSTN 9-1-1 network and provides locator information and stores ANI data for all the phones on the Ames campus. The Telident system is located in Building N263.

The ARC Dispatch Office serves as the Public Safety Answering Point (PSAP) for ARC where the information from the Telident is displayed. The AT&T Positron 9-1-1 call management system is currently being switched to a Zetron system.

4.1.17.5 Analog Phone and FAX Services

FAX and analog services are provided by the services support contract and set up from the Northern Telcom, SL-100 switch.

There are approximately 2400 active analog lines. These lines are used for FAX machines, conference phones, and single-line analog sets.

4.1.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.1.19 Cable Television Services

The Ames Cable television distribution infrastructure is a coaxial cable plant that distributes 24 channels of content throughout the Center. Sources range from four different NASA TV feeds, local, cable news stations, Stanford Instructional Television programming, as well as local productions.

4.1.20 Continuation of Center Zoned Architecture Project (CZAP)

The ARCLAN currently supports a zoned architecture. This architecture can be transitioned to the proposed NASA NCI network architecture. Some systems and networks will have to migrate between zones based on access requirements. These system migrations will occur prior to NICS contract transition. Overall system managed for network infrastructure will be consistent with current levels of support.

4.1.21 Ongoing Center-Specific Projects

ARC is currently in the planning stages of a new “green” administrative building. This will be a multi-floor building with full wired and wireless capabilities. Sensors will be installed through the building on the network for environmental monitoring of the efficiency of the building.

In 2008, ARC conducted a pilot of VoIP technology, to evaluate three vendor systems (Shoretel, Cisco, and Avaya) as possible candidates for ARC telephone system replacement.

4.1.22 Work Load Indicators

Trouble tickets are currently managed by a local helpdesk.

4.1.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.2 DRYDEN FLIGHT RESEARCH CENTER (DFRC)

Dryden Flight Research Center is located on Edwards Air Force Base (AFB) in Southern California. Currently, DFRC supports approximately 1400 total users, dispersed between approximately 70 individual buildings and two remote facilities. Approximately 200 of those users work at one of the two DFRC remote facilities located in Palmdale, both of which are located about 45 minutes north of the Dryden campus. Both remote Dryden facilities rely on network services located on the primary Dryden campus. The Dryden network supports approximately 3800 network devices including Cisco Voice over IP phones.

4.2.1 Property/Inventory

The contractor provides network operations and maintenance for all components of the Dryden network infrastructure. NICS RFP Attachments J-8, *Government Furnished Property*, and J-9, *Installation Accountable Government Property* is the definitive list of equipment the contactor will be responsible for shipping/receiving/inspection.

4.2.2 Shipping/Receiving/Inspection

DFRC has centralized shipping and receiving warehouse, contractors should utilize this facility.

4.2.3 Vehicles Necessary To Support Center Work

The contractor will not be provided any dedicated vehicles. Government vehicles are available for checkout, from the DFRC motor pool, if required.

4.2.4 Physical Safety

The contract must adhere to the safety policies and procedures of DFRC.

4.2.5 Emergency Management

The Dryden Emergency Operations System provides wireless and voice services in the event of disaster that renders the standard DFRC network unusable. The system includes a satellite system, a wireless LAN controller and network infrastructure.

4.2.6 Safety

The contract must adhere to the safety policies and procedures of DFRC.

4.2.7 Facilities

The NICS personnel will be allocated space within Building 4838 of Dryden Flight Research Center. The following is a listing by type of space.

Type of Space	Square Footage
Office Space	1400
Storage	1000

Lab	100
Conference Room	500
Miscellaneous	500

4.2.8 Network Services

4.2.8.1 IPAM

4.2.8.2 Remote Access

Remote Access Services for DFRC clients include client-based VPNs terminated on a Cisco 5520 ASA VPN concentrators for IPSec based VPNs. In addition a Juniper Neoteris SSL VPN is provided.

4.2.8.3 NTP

Information to be provided by Center, not yet available.

4.2.8.4 Guest Network Services

The Dryden and DAOF Extranet zones offer wired guest connectivity if required by end-user. Guest wireless services are available at all three (3) Dryden physical locations. All wireless Guest network services are managed by Cisco Wireless LAN Controllers located in the Dryden Data Center.

4.2.9 Data Services

4.2.9.1 High Level LAN Description

The Dryden network consists of the standard core, distribution and access layers. The core and distribution layers consist of Cisco 6500 Multilayer switches; the access layer consists primarily of Cisco 3750 workgroup switches.

There are currently five network zones within the DFRC campus: Dryden Intranet, Dryden Extranet, Dryden Public, Dryden Server and Dryden Security Command Center. A high level descript of the network zones is as follows:

a) Dryden Intranet Zone

The Dryden Intranet network zone provides intra-campus system connectivity that supports approximately 3500 devices located within the Dryden and DAOF campuses. The AeroInstitute will be transitioned to the Dryden Intranet as part of the NASA NCI project. The Dryden Campus currently consists of fifteen Distribution Layer Switches, two Core Layer Switches, and approximately one hundred dedicated access layer switches. The DAOF Local Area Network supports approximately 200 network devices and consists of one core

switch, four distribution switches, and approximately 24 dedicated access layer switches. The Dryden intranet is a converged network supporting voice, video and data services. The Dryden Intranet network zone provides a layer 3 backbone that supports 1Gbps and 10Gbps connections between distribution points and core routers. The layer 3 routing protocol implemented within the campus is Cisco's EIGRP routing protocol. The Dryden Intranet network zone supports Layer 2 connectivity at all locations within the campus at speeds of 100Mbps or 1Gbps connectivity depending on cabling and infrastructure device capabilities. Network separation is provided via static Virtual Local Area Networks (VLANs), campus VLANs were created for:

1. Server VLANs – VLAN to support Dryden campus server connectivity (Server Zone).
2. User VLANs – Located at all Distribution points within the Dryden and DAOF campus locations, these VLANs support general client connectivity.
3. Voice VLANs – Located at all Distribution points within the Dryden and DAOF campus locations, these VLANs support Voice over IP client connectivity.
4. Printers – Located at all Distribution points within the Dryden and DAOF campus locations, these VLANs support printer connectivity.

The Dryden Intranet and DAOF Intranet are connected by NISN managed Wide Area Network connections. The DAOF Intranet utilizes network services from the Dryden campus.

b) Dryden Extranet Zone

The second network zone within the Dryden Local Area Network is the Dryden Extranet. The Dryden Extranet utilizes physically separate network cable and infrastructure from other Dryden network zones. This infrastructure provides data connectivity for specific projects or NASA partners that have security or connectivity requirements that differ from the standard Dryden campus. The Extranet network backbone consists of a series of layer 2 networks that are routed by an IT Security managed Extranet Firewall, because the network is layer 2 each network can be distributed to multiple physical locations within the campus. The Dryden Extranet is located at all three major Dryden Locations: AeroInstitute, DAOF, and the Dryden Campus. Connectivity between the Dryden Extranet with the remote facility Extranets is support through NISN managed Wide Area Network connections. The primary components of the Dryden Extranet are 3750 workgroup switches; these switches act as the distribution and access layer for this network. Individual projects are separated on the Dryden Extranet using VLANs; these VLANs are then routed by the Dryden Extranet firewall. The Dryden Extranet also hosts the Dryden Wireless Infrastructure, Wireless Local Area Networks and the Dryden Emergency Operations Center. The Dryden Extranet is located on the DFRC perimeter network and is protected by IT Security managed Juniper NS-500 clustered firewalls.

c) Dryden Public Zone

The Dryden Public server zone is an isolated network located physically in the DFRC Data Center. This network hosts systems that are accessible from the Internet and offer Public Services. These devices include Remote Access devices, FTP servers and web servers.

d) Dryden Server Zone

The Dryden Server zone is physically part of the Dryden Intranet. There are currently two designated server zones within the Dryden Intranet: the DFRC Server Farm and the DAOF Server Farm.

e) Dryden Security Command Center (SCC) Zone

The third network zone within the Dryden Local Area Network is the Security Command Center network. This network supports physical security systems and uses physically isolated cables to support connectivity. Internet connectivity is provided through IT Security managed firewalls; the external firewall interface is connected to the DFRC Intranet zone. The network backbone consists of Cisco 2950 workgroup switches configured using a layer 2 backbone. The Dryden campus SCC network is located in five DFRC buildings; the DAOF SCC network is located within Building 703 of the DAOF campus.

4.2.9.2 Wireless Networks

The Dryden Wireless infrastructure is implemented on the Dryden Extranet Zone and supports wireless client connectivity and the wireless management network. The Dryden wireless network infrastructure consists of a secure Wireless LAN and a guest Wireless LAN.

The Dryden wireless infrastructure consists of:

a. Centrally managed Cisco Wireless Access Points that provide wireless services to end users
b. Cisco Wireless Management and monitoring systems
c. AirMagnet wireless management devices - these systems will be located within the Dryden infrastructure and do not offer wireless services. These devices are passive wireless monitoring, reporting, and security devices.

Wireless services are consistently provided among all three DFRC network locations: Dryden campus, AeroInstitute, and DAOF. Dual Cisco Wireless LAN controllers exist on the Dryden Extranet network and manage Cisco Access Points at located at all three locations.

4.2.9.3 Network Security

The Dryden Intranet is further segmented by utilizing IT Security managed internal firewalls. All Dryden firewalls are centrally managed and monitored by IT Security operations. Currently there are six intranet firewall systems:

a) Simulation Lab Firewalls: Cisco Firewall Services Module

These clustered Cisco Firewall Services Modules provide access control for DFRC simulation servers. The network infrastructure in the simulation lab is considered part of the Dryden Intranet zone. The simulation lab firewalls supports systems that are part of the Dryden Flight Simulation projects, this system is considered to flight operations at Dryden.

b) AeroInstitute Firewall : Cisco PIX 515

The AeroInstitute Firewall provides access control services for the AeroInstitute remote facility. The AeroInstitute firewall provides network segmentation for AeroInstitute wireless infrastructure, Educational Video collaboration equipment and clients. The network infrastructure at the AeroInstitute is considered part of the Dryden Extranet, but will be transitioned to the Dryden intranet during the NASA NCI project.

c) IT Security: Sun Ultra 60 Checkpoint Firewall/Cisco PIX 515

The IT Security Firewalls provide access control for IT Security support systems. These systems include: Intrusion Detection Systems, log servers and Security Incident Management servers. The IT Security network infrastructure consists of Cisco 3750 Workgroup switches and is considered part of the Dryden intranet.

d) DAOF Firewall: Cisco PIX 535

The DAOF firewall provides the boundary between the DAOF network infrastructure and the NISN WAN that connects the DAOF network to the Dryden Campus Intranet. These firewalls also provide the boundary for the DAOF Security Command Center Network and the Dryden Intranet.

e) Flight Loads Lab Firewalls: 2 Juniper Netscreen SSG5s

The Flight Loads Lab (FLL) firewall provides transparent firewall services to isolate Flight Loads Lab test equipment. The FLL firewalls are required to minimize network impacts to and from the Dryden intranet to the FLL test systems. The FLL network infrastructure consists of non-managed hubs that are considered part of the Dryden intranet.

4.2.9.4 Network Operations

Network operations services are hardware and software applications that provide monitoring and management services for the network infrastructure. Currently the hardware implemented includes Dell Hardware and Apple Hardware.

Network Management software implemented includes:

a. Intermapper – network system monitoring and visual alerting
b. NetQOS – network performance/trend analysis tool
c. SolarWinds – network polling and system alert generation
d. AirMagnet – wireless system monitoring

A single instance of each network management package is used manage all Dryden network zones. Network management displays are available via web browser and are also displayed in the Dryden Network Operations Center. The Dryden Network Operations Center is located in building 4838 and provides displays for network management/monitoring hardware. The NOC supports seating for approximately five personnel.

4.2.9.5 Network Processes

Configuration and change management for all network infrastructures is governed by the Dryden IT Infrastructure board. This board is governed by the Dryden Deputy CIO and manages the configuration for all Dryden IT infrastructures.

4.2.9.6 Network Lab

Dryden has a network lab created to support integration and upgrade testing. The Dryden network lab consists of replicas of DFRC backbone switches, wireless hardware and VoIP hardware and software.

4.2.9.7 Hardware Description

The following hardware platforms are utilized to create the Dryden network and security architecture.

Quantity	Make & Model	Function
120	3750-24 Switches	Access Layer devices with the Dryden, DAOF and AeroInstitute campus networks
4	3750-12 Switches	Backbone devices for DFRC Extranet zone
30	3750-48 Switches	Access Layer devices with the Dryden, DAOF campus networks
19	6500Multilayer Switches	Core and Distribution points within the Dryden and DAOF networks
2	3660 Routers	AeroInstitute GRE Tunnel; will be phased out during NCI transition

Quantity	Make & Model	Function
8	3550 Switches	Access Layer devices within the Simulation Network
10	2950 Switches (will be phased out)	Security Command Center network infrastructure; will be replaced by Cisco 3750 switches in the future.
2	4404 Wireless LAN Controllers	Production Wireless LAN Management Systems
1	4402 Wireless LAN Controller	Lab Wireless LAN Management System (used for testing)
1	3750 Switch with integrated Wireless LAN Controller	Emergency Operations Center Wireless LAN management System
50	1240Wireless Access Points	Managed Wireless Access Points
5	Dell 5224 Switch	Simulation Lab access Layer
10	Dell 5324 Switch	Simulation Lab access Layer
3	Nortel 450 switch	Simulation Lab access Layer
6	Firewall Services Module (6500 Blade)	Lab systems, Simulation Lab firewall and WATR Firewall
1	Intrusion Detection Services Module (6500 Blade)	Server Farm Intrusion Detection System
11	CEF720 24 port 1000mb SFP Module (6500 Blade)	1 GB fiber connectivity from Dryden Distribution Points
30	Supervisor Engine 720 (6500 Blade)	Cisco 6500 Supervisor blades
6	CEF720 48 port 10/100/1000mb Ethernet module (6500 Blade)	Server Farm copper connectivity blade
18	CEF720 4 port 10-Gigabit Ethernet module (6500 Blade)	10GB Fiber connectivity backbone
45	SFM-capable 48 port 10/100/1000mb Ethernet Module (6500 Blade)	End-user/phone connectivity to Cisco 6500 Distribution points
2	Juniper Neoteris SSL Gateways	SSL VPN Portal
1	Cisco ASA 5520 VPN Concentrator	IPSEC VPN Concentrator
2	Cisco PIX 535	DAOF Network Firewall
3	Checkpoint Software based firewall (will be phased out)	Current Intranet and IT Security Networks Firewalls
6	Juniper Netscreen Firewalls model SSG	Flight Loads Lab and Remote Access Network Firewalls
2	Juniper Netscreen Firewalls model: NS-500	DFRC Extranet Firewall
2	Juniper Netscreen Firewalls	Security Command Center Firewall

Quantity	Make & Model	Function
	model: NS-204	

4.2.9.8 Hardware Refresh

Information to be provided by Center, not yet available.

4.2.10 Collaboration Services

4.2.10.1 ViTs Rooms

DFRC has the following ViTS Rooms:

Location	Bldg #	Room #	Room Description
DFRC	4801	2221	DFRC 1 MAIN CORE ROOM
DFRC	4802	2702	VITS ROLL ABOUT (VRA) MOVEABLE SYSTEM
DFRC	4838	120	DAF CONF ROOM
DFRC	4839	PACE OFFICE CONF ROOM	VRA SYSTEM
DAOF	703	PILOTS OFFICE 1ST FLR N.	VRA SYSTEM -A.K.A. ARCTAS CONF ROOM
DAOF	703	TRANSTION CONF ROOM 1 ST FLR S.	VRA SYSTEM- MOVED TO UNKNOWN LOCATION BLDG 703 S.

4.2.10.2 Conference Room Support

The contractor will provide and support IT infrastructure in designated conference rooms within the Dryden and DAOF campuses

4.2.11 Customer Relationship Management

Information to be provided by Center, not yet available.

4.2.12 IT Security

Information to be provided by Center, not yet available.

4.2.13 Cable Plant Services (RESERVED)

4.2.14 Emergency Warning Systems (RESERVED)

4.2.15 Public Address System (RESERVED)

4.2.16 Radio Services (RESERVED)

4.2.17 Telephone Services (RESERVED)

Dryden primarily utilizes Voice over IP for standard phone service, however, a limited number of analog phones and phone services are still available.

4.2.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.2.19 Cable Television Services (RESERVED)

4.2.20 Continuation of Center Zoned Architecture Project (CZAP)

The Dryden network currently supports a zoned architecture; this architecture will transition seamlessly with the proposed NASA NCI network architecture. Some systems and networks will have to migrate between zones based on access requirements. These system migrations will occur prior to NICS contract transition. Overall system managed for network infrastructure will be consistent with current levels of support.

4.2.21 Ongoing Center-Specific Projects

4.2.21.1 Dryden Data Center

Dryden is currently building a new building to support a new Dryden Data Center. All IT infrastructures from the current data center will have to be re-located to the new data center. The current schedule for completion of the building is fourth quarter of 2010 and occupancy could begin in 2011. The contractor will be required to support migration of existing network hardware from current data center to new data center.

4.2.22 Work Load Indicators

PWS Section	Indicator	Approximate Quantities/month
3.1.1	IPAM data updates	~20
3.1.2	New or updated remote access accounts	~20
3.1.4	Number of guest accounts	~40
3.6	Network trouble tickets	90 (trouble tickets, service requests and moves all reported under a single total)

3.6	Network moves, adds, changes	See above
3.6	Network service requests	See above
3.12	IT security incident response support	~12 (includes SOC requests and system analysis requests)
3.12	Firewall rule changes	~30
3.12	Security documentation packages	25
4.x.5	Telephone trouble tickets	N/A
4.x.5	Telephone moves, adds, changes	N/A
4.x.5	Telephone service requests	N/A
5.0	Network projects greater than $500K	0

4.2.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.3 GLENN RESEARCH CENTER (GRC)

The Glenn Research Center at Lewis Field (GRC) is situated on 350 acres adjacent to the Cleveland Hopkins International Airport. It has more than 140 buildings that include 24 major facilities and over 500 specialized research and test facilities. In addition, Plum Brook Station (a.k.a. PB), located 50 miles west of Cleveland in Sandusky, offers four large, world-class facilities for space technology and capability development on a 6,400-acre site.

The Glenn workforce, spread throughout GRC and PB, is made up of more than 3,000 civil service employees and support service contractor personnel. Scientists and engineers comprise more than half of the workforce and are supported by technical specialists, skilled workers, and an administrative staff. Their work is focused on technological advancements in spaceflight systems development, space propulsion, aero-propulsion, power systems, nuclear systems, communications, and human research.

All Glenn capabilities are available for government and industry programs through interagency or Space Act agreements. Relationships have been established with such partners as the Cleveland Federal Executive Board (FEB), the Ohio Aerospace Institute (OAI), and residents of the Aerospace Technology Park (ATP). The FEB is located in downtown Cleveland and the OAI and ATP are located just outside GRC's west gate.

4.3.1 Property/Inventory

The Agency nProp system is used to manage property at GRC. The GRC Logistics and Technical Information Division (LTID), Code CO00, is the property management organization. The NICS contractor will work with LTID and its support contractors to determine the best tool and methodology to manage property under the responsibility of the NICS contract.

4.3.2 Shipping/Receiving/Inspection

The NICS contractor will be responsible for shipping, receiving, inspection, acceptance, and storage of equipment. The contractor will make arrangements with LTID for equipment tagging and the excess of equipment.

4.3.3 Vehicles Necessary To Support Center Work

Communications services personnel routinely use commercial vans to support their onsite activities and to transport personnel and equipment between Lewis Field and Plum Brook. These vans are not furnished by the Government.

At Lewis Field, a lab bus is available to transport all personnel on the main Lab only. The bus runs from 7:45 a.m. to 4:30 p.m., Monday through Friday. In addition, an airport courier service

is available for NASA personnel and resident contractors who are on official business and need 24-hour transportation to Cleveland Hopkins Airport. A motor vehicle pool provides official travel support for civil service employees and on-site contractors. The pool is operated on a first call basis from 7:00 a.m. to 4:00 p.m. daily. Sedans, minivans, and a small cargo van are available.

4.3.4 Physcial Security

The GRC Office of Protective Services is responsible for physical security at both Lewis Field and Plum Brook Station. Its guard force handles a variety of tasks including the issuing of badges, the processing of visitors, vehicle inspections, responding to life, safety, and security alarms and situations, traffic management, and ground patrols.

All contractor personnel having a need to enter areas of the Glenn Research Center's Lewis Field or Plum Brook Station must possess an identification pass or badge. This badge or pass is obtained at the main entrances to the facilities. During normal working hours, the guards at the gates will permit contractor entrance and departure. At any other time, advance clearance is required. Firearms or weapons of any kind are strictly prohibited. Emergency, Fire, Medical, Safety, and Security assistance can be summoned by dialing "911" on the Center's PABX telephone system.

4.3.5 Emergency Management

The GRC Emergency Preparedness Office is responsible for emergency management at both Lewis Field and Plum Brook Station. It oversees the NASA GRC Evacuation Plan which provides general guidelines to evacuate Center personnel, contractors, and visitors in times of emergency. The GRC Emergency Management Coordinator is the maintainer of this plan. Depending on the nature of the emergency, an Emergency Operations Center (EOC) may be established to serve as the focal point of the evacuation process and subsequent emergency requirements. Until the Center EOC is established, the Emergency Dispatch Center functions as the EOC. In the event of an emergency, notifications will be made through a variety of means including, but not limited to, the Center's telephone system, the radio communication system, Information Technology (IT) computer systems, and the Lewis Information Network (cable television).

4.3.5.1 Center Specific COOP Support

GRC has developed a COOP plan, managed out of the Security Management and Safeguards Office (SMSO). Various GRC organizations and their supporting contractors provided input to this plan. The current GRC IT provisioning contracts, ODIN and PACE, are responsible for supporting ongoing revisions to the IT sections of the GRC COOP plan. As IT work elements are moved into NICS, responsibility for GRC COOP support will transition as well.

4.3.5.2 Service Continuity of Operations Support

The ODIN and PACE contracts provide the necessary staffing to support any required IT service continuity of operations at GRC during common scenarios such as severe weather (e.g. winter storms) or other events as circumstances warrant. As IT work elements are moved into NICS, responsibility for GRC IT service continuity will transition as well.

4.3.6 Safety

Site specific health and safety plans are required in the execution of work on the communications infrastructure to help identify and control potential hazards such as: lead, asbestos, electric shock, confined spaces, fall hazards, and noise. Deviations from these plans can result in an order to stop work. Permits and work plans are required for events such as the use of lasers, lifting devices and cranes; for confined space and electrical substation entry; and excavations. Special training and personal protective equipment are routinely required and could include the use of safety glasses, hard hats, boots, gloves, and hearing protection. Glenn adheres to all health, safety, and environmental rules and regulations. In addition, OSHA has the right to visit and inspect construction activities.

4.3.7 Facilities

At GRC, three buildings serve as the main hubs for all communications services. Building 142 houses central servers, mass storage systems, and also serves as the hub for the Center's video distribution system. The Glenn Network Operations Center (GNOC) and telephone switchboard are also located in building 142. Building 322 houses the WAN gateway and firewall that connect Glenn to the Internet and NISN (the Agency Intranet). Current plans call for relocating all communications equipment from Building 322 to Building 142, leaving Building 322 as a passive cabling hub for GRC's west area buildings. Finally, Building 15 houses the telephone system(s) and all equipment necessary to connect GRC to local and national telephone systems.

Communications services personnel are housed in each of the three buildings and in Building 21. The office space designated for their use is tabulated below. Please note, the square footages shown for Building 142 include future space required for the Building 322 relocation effort.

Building	Office Space (sq. ft.)	Non-Office Space (sq. ft.)
15	194	1573
21	60	0
142	1965	2406
322	285	2938

Two buildings serve as the main communications hubs at Plum Brook Station. Building 7233 houses the telephone switch and all equipment necessary to connect to local telephone services, and the equipment that connects the phone and network systems between Plum Brook Station and Lewis Field. Building 7141 is the hub for all Plum Brook Station network systems.

4.3.8 Network Services

4.3.8.1 IPAM

As of the release of this RFP, GRC had not yet transitioned to the Agency IPAM service. Transition is anticipated to occur in May 2009. When transition is complete, GRC will have 3 Agency IPAM servers providing DNS and DHCP services to users. These servers will be located in Building 142 (data center) and Building 15 (telephone switch room).

4.3.8.2 RAS

Dial-in services are provided by the Center's Remote Access Service (RAS) system deployed in the late 1990's. Through the use of the Public Switch Telephone Network (PSTN), RAS enables authorized personnel to establish a communications link between their computer system/modem and the GRC network, making the computer appear as a host node on the network. Both local and toll-free telephone access to the Center is supported. Call routing, administration, authentication, authorization, accounting, customer support, and technology enhancements are all elements of the RAS system.

The primary RAS component is a Cisco Systems' AS5300 Universal Access Server located in the Building 15, Telephone Switch room. An Integrated Service Digital Network – Primary Rate Interface (ISDN –PRI) line enters the Center and terminates at this server. Configuration of the PRI allows for a maximum of 23 analog (56Kbps) connections or, a combination of analog and ISDN connections. The AS5300 has a Quad PRI/TI card and eight 6-port Modem Modules containing 48 Digital/Analog Modem ISDN Channel Aggregation (MICA) Modems ITU Standard V.34, V.90 56Kbps.

A 100Base-TX Ethernet port on the AS5300 connects the access server to a Cisco Catalyst 3524XL switch with a Gigabit uplink to a GRC core switch. Located in a nearby rack, and connected to this 3524XL switch, is the server used for RAS authentication, authorization, and accounting. A Network Management Station housed in the GNOC is used to manage and monitor the AS5300 access server.

Out of a pool of over 1300 RAS users, the service is currently experiencing loads of approximately 12 to 20 concurrent users during prime time periods.

In addition to dial-in service, GRC currently uses the Juniper SA 6000 appliance to provide Virtual Private Network (VPN) services to authorized users. Two redundant appliances, each connected to the GRC network at Gigabit Ethernet speed, can support 5000 concurrent users. However, as of December 2008, the actual number of concurrent users is limited to 100 due to software licensing. A valid userid and 2-factor (SecureID token) authentication are required to access the GRC internal network via VPN.

4.3.8.3 NTP

GRC currently provides Network Time Protocol service with redundant servers.

4.3.8.4 Guest Network

GRC has two wireless networks. One network services provides secured and encrypted wireless access to the GRC internal network. It is intend for use by onsite civil service employees and support service contractors. The other network, GRCguest, is intended for visitors to the Center. The Guest Network is unsecured and unencrypted. The same access points provide both guest wireless and wireless access to the GRC internal network as described in Section 4.3.9.2, Wireless Network below.

4.3.9 Data Services

4.3.9.1 High Level LAN Description

The GRC network is based on a switched Gigabit, full duplex Ethernet architecture (circa late 1990's). There are four Cisco 6509 switches, each with redundant power supplies and processor cards. The four switches, called the network core, are interconnected via single mode fiber optic cable in a fully meshed topology. Each switch is powered thru an uninterruptible power supply with three of the four switches having generator backup. In addition to the network core, eight Cisco 6509 LAN switches serve as a distribution layer.

The core switches are placed in strategic locations across Lewis Field. A switch in Building 5 serves the North Area and a switch in Building 15 serves the central portion of the main campus. The third switch in Building 142 serves central servers, offices in that building, and other nearby buildings, including those that are south of K-Road. A fourth switch in Building 322 connects to the Internet, the NASA Agency-wide network and also serves the West Area, including the OAI and Aerospace Technology Park. When all equipment is moved out of Building 322, the fourth core switch will move to building 142. All core switches are interconnected to building networks and servers by means of the Center's fiber "backbone" as described in Section 4.3.13 Cable Plant Services.

Each of the four core switches are configured differently through the use of Gigabit Ethernet or 10/100 Ethernet interfaces. Various building and special purpose networks are attached to these interfaces. Although present building networks can be Coax (10base2, 10base5), shared 10baseT, or switched 100baseT, plans are underway to upgrade the entire network at GRC to allow for 100Mb/1Gb to every desktop. See Section 4.3.21, Ongoing Center-Specific Projects. In its current configuration, the GRC LAN supports approximately 5,000 IP addresses.

Plum Brook does not have a network core. A single Cisco 6509 switch located in Building 7141 serves as the hub for all PB network systems. This switch is connected via a DS-3 to GRC, extending GRC's IP address space to Plum Brook with about 200 IP addresses. This switch is not equipped with battery or generator backup. Building LANs at Plum Brook are similar to those at GRC.

4.3.9.2 Wireless Networks

The GRC Wireless LAN (WLAN) network is based on the 802.11g Cisco model 1200 access points. The current WLAN architecture uses Power over Ethernet (POE) switches on the GRC External Services Network (ESN). These switches are trunked back to the GRC core switches for routing purposes. Each access point provides both guest wireless and wireless access to the GRC internal network. Guest wireless is unsecured and unencrypted. A valid userid and 2-factor (SecureID token) authentication are required to access the GRC internal network. Users authorized to access the GRC network via wireless are provided data encryption.

Presently, wireless access points are located in common areas (e.g. conference rooms and lobbies) of buildings 3, 4, 5, 6, 7, 8, 15, 16, 21, 23, 49, 50, 54, 55, 60, 77, 86, 105, 106, 110, 142, 143, 145, 301, 302, 309 and 333. Some buildings have additional WLAN coverage beyond the common areas. Building 7141 is the only location at Plum Brook to offer WLAN service.

4.3.9.3 Network Security

Information to be provided by Center, not yet available.

4.3.9.4 Network Operations

The Glenn Network Operations Center (GNOC) provides second and third level help desk support for all network related matters at GRC and Plum Brook. The GNOC is responsible for monitoring, problem resolution, change control, configuration, and documentation. It is staffed Monday thru Friday, 7:00am – 5:30pm with 24 x 7 x 365 support via an on-call pager.

GNOC personnel perform routine maintenance and upgrades; provide engineering support for research, planning, and integration of new network services; administer VPN and RAS accounts;

and perform updates to the Glenn TV (GTV) video bulletin board. The GNOC also supports the GRC video head-end.

A number of tools are used by the GNOC to monitor and manage the network. They include, but are not limited to: WhatsUp Professional; Denika trend tracking; CiscoWorks2000; InterMapper; PING; Traceroute; NSLookup; Network Associates Sniffer Pro; and AirMagnet.

The GNOC also maintains documentation in an eRoom where configuration information and drawings are stored. Drawings are in Visio and AutoCAD, depending on the documentation requirement. Digital JPEG images are also maintained of racks in communications rooms.

4.3.9.5 Network Processes

Information to be provided by Center, not yet available.

4.3.9.6 Network Lab

Information to be provided by Center, not yet available.

4.3.9.7 Hardware Description

The Hardware used in the GRC Local Area Networks is largely Cisco Systems based routers and switches. A few legacy Cabletron shared hubs remain in service as does some hardware to support the remaining coax-based Ethernet cable. The firewall is a Juniper 5400. Additional detailed equipment lists will be made available during the NICS due diligence period.

4.3.9.8 Hardware Refresh

There are no standard hardware refresh cycles at the Glenn Research Center due to an on-going lack of adequate funding. Hardware is refreshed when it a) can no longer be supported, b) no longer supports the connectivity requirements it must satisfy and c) funding has been identified and made available for this purpose.

4.3.10 Collaboration Services

Information to be provided by Center, not yet available.

4.3.11 Customer Relationship Management (CRM)

The following table contains network demarcation information and “touch points” to other local area networks at the Center.

Network Name	Provider	Description
NASA Safety Ctr. @ Ohio Aerospace Institute (OAI)	Dedicated fiber controlled by GRC	Use of NASA IP Address Space NASA extends network to this near site facility (OAI) that houses NASA personnel and support staff for the NASA Safety Center.
Federal Executive Board (FEB)	ICG	Use of NASA IP Address Space Off-site (Cleveland, OH) facility – NASA GRC provides network services to this Government agency.
Plum Brook Station (PBS)	DS-3 provided by NISN	Use of NASA IP Address Space Extension of GRC LAN to PBS located 60 miles west of Cleveland. NISN provides the circuit and ODIN manages the end equipment.
Tele Science Center	NISN Premium IP	15 Mb dedicated Line on NISN premium IP
LMIT(ODIN)	Dedicated fiber	Use of NASA IP Address Space Near site facility (Aerospace Tech. Park)
General Electric (GE) Cincinnati, OH	T1-NISN	NISN provided services to test facility at this remote location
Pratt & Whitney Hartford, CT	T1-NISN	NISN provided services to test facility at this remote location
Various Test Facilities LANS	Internal fiber provided by ODIN	Use of NASA IP Address Space Network services to data acquisition systems in GRC test facilities.

4.3.12 IT Security

Information to be provided by Center, not yet available.

4.3.13 Cable Plant Services

All GRC buildings are attached to a common set of interconnecting pathways. The common set of interconnecting pathways utilized by the communications cabling infrastructure at the Center

include systems of underground manholes, ducts, tunnels, cable trays, guide wires, telephone poles and direct burial. These communications pathways generally follow a "tree-like" configuration. This means that some buildings only have a single path to one other building, while other buildings have various paths, each to a separate building. This does not preclude the fact that there are loops within the pathways, or possible multiple paths between some buildings. The inter-building cabling infrastructure utilizes this common set of interconnected pathways to get from one building's demark point to another building's demark point.

Between GRC buildings the usual pathway is through a system of buried ducts and manholes. This manhole system is dedicated to telecommunications and low voltage cabling, thus it is commonly referred to as the "telephone manhole system". No other utilities (i.e., electricity, natural gas, or water) are within this system. The manholes of this system include various sizes and shapes, some of which are actually hand-holes. The locations of the personnel access openings of these manholes are mostly within grassy areas, although a few are in paved parking areas or within a building (i.e., building 15 and building 21). Within the manhole system there are drains for water, but some are still at times filled with non-potable water that must be pumped-out prior to entry.

From this telephone manhole system, there are ducts that reach most of the buildings. Due to the variety of the facilities at the Center, the place these ducts reach the buildings also varies. Some of the areas where the cables enter the building could be secured, locked, have limited access, or in an area with potential hazards.

At Plum Brook Station, telephone poles and direct burial cable are used in the deployment of the communications cabling infrastructure. Plum Brook Station does not have a dedicated "telephone manhole system".

The GRC core switches connect to building networks and servers at speeds ranging from 10 Megabit to 1 Gigabit. The interconnection from the core to buildings and servers is multimode or single mode fiber cabling, depending on distance (single mode accommodates longer distances). Within the Center's buildings and concentrated server areas, the typical connection media is Category 5/5E, Unshielded Twisted Pair (UTP) cable operating at 10Mb or 100Mb. There are also small pockets of older coax-based network cabling, limited to a 10Mb speed. All connections are Ethernet based using the TCP/IP protocol.

The communications cable infrastructure at Plum Brook Station is a combination of copper and fiber. Cable plant services required are the same as those required at GRC, except the majority of this cable is direct buried, with a small amount that is aerial.

4.3.13.1 Optical Fiber

At Lewis Field, multimode fiber optic cables are 62.5/125 microns with a 1300 nm (nanometer) window and LED (Light Emitting Diode) light source (preferred). Single mode fiber is 8/125 microns using the 1310 nm (nanometer) window and a laser source (preferred). Typical practice is to install the fiber in orange duct liner to prevent damage. The liner is then secured to guide wires, cable trays, or any similar structure such as girders available within the ceiling or other structural components. Pull boxes are also used to protect the fiber optic cable from micro-bends. The fiber optic cables are not spliced within any of the Center's manholes.

4.3.13.2 Twisted Pair Copper Cabling

Ethernet UTP Cable is 10/100BaseT Unshielded Twisted Pair (UTP), with both plenum and non-plenum ratings, depending on application. The minimum specification is Category 5 with characteristic impedance 100 ohms, +/- 15 ohms. It utilizes 4-pair twisted cable and terminates in a standard RJ45 8-pin modular jack with EIA/TIA 568 pin configuration (AT&T 258A) at the wall plate and Category 5 (or better) rated patch panels in the wiring closets. All cable is installed in cable trays (preferred), J-hooks, rings, conduits, etc. with proper installation techniques for a Premises Distribution System (PDS) architecture. Most of the Center's existing buildings are cabled with Category 5, but new installations are Category 5E cabling, rated for speeds up to 1 Gigabit. There are a few buildings that have Category 3 cabling, which can only accommodate 10Mb Ethernet speeds.

4.3.14 Emergency Warning System (RESERVED)

4.3.15 Public Address Systems (RESERVED)

4.3.16 Radio Services

GRC 2-way radio service is provided via a Motorola Astro Digital Radio System located in Building 110. The site has a generator for backup power. This system was activated in 2007 and went into full production in February 2008 to comply with the NTIA narrow band mandate. Approximately 25 base stations are in use along with 200 portable units. There are no mobile units mounted in vehicles.

While the GRC Office of the Chief Information Officer (OCIO) manages the radio service via the ODIN contract, frequency management is outside of the OCIO and is performed by the RF Spectrum Manager who resides in the Engineering Directorate (Code D). The GRC RF Spectrum Manager must be contacted to obtain prior approval before procuring, accepting, or installing any type of RF equipment for use at Lewis Field and Plum Brook Station.

Plum Brook Station utilizes the Multi Agency Radio Communications System (MARCS) to provide 2-way radio service for its safety and security forces. Approximately 20 portable units are in use along with five (5) mobile units, some of which are mounted in vehicles. Radio service for research facilities and logistics/operations personnel are provided thru a pool of legacy 2-channel radios. The OCIO is currently working with Plum Brook to replace this pool with a modern digital system similar to the one in use at the GRC campus.

4.3.17 Telephone Services

The heart of the GRC telephone system is a Fujitsu F9600XL telephone switch (circa 1990) installed in Building 15. It is fully redundant down to the line card-level. In its current configuration, the F9600 currently supports approximately 3000 analog telephones and 1500 digital telephones.

The GRC telephone switch, voice processing system, and all associated equipment are powered through an uninterruptible power supply (UPS) system. The UPS consists of batteries, a transfer switch, and a natural gas generator that keeps the telephone system running at full capability should commercial power fail. The UPS system is tested on a monthly basis. The tests are performed by a Lewis Field onsite contractor with the assistance of the telephone service provider.

The majority of cable that supports the GRC telephone system is industry standard copper telephone cable of 19, 22, or 24 gauge. Bundle sizes range from single pairs that serve individual phones to 1200 pair serving major buildings.

Many splices reside in the GRC telephone manholes and connect together in multiple ways. As a result, a large bundle of cable can enter a manhole from one direction and exit out in many different directions in smaller bundles of cables. The copper is spliced point-to-point, that is to say, for a single copper wire it is only terminated in two areas, one for each end. There are no multi-drop-spliced cables. There is some cable that terminates in a splice (i.e., the cable enters a manhole but does not leave through another). The cable enters a building and is terminated into a lightning suppressor.

A Fujitsu F9600ES Telephone switch (circa 1997) provides telephone services to Plum Brook Station. The F9600ES system is located in Plum Brook Building 7233. The site has neither battery nor generator backup for electrical power. The system has a capacity for 400 phones and currently supports 150 analog and 150 digital telephone station ports.

4.3.17.1 Handsets

A variety of telephone sets are in use at both GRC and PB including analog and digital, single line, multi-line, and conference phones, speaker and display (caller ID) models, wall mount and

desktop styles. Most models of phones supports last number redial, speed calling, call transfer, call forward, call-park, storage of numbers, and 3-way conferencing. Fujitsu Multi-Line Digital Telephones (MLDT's) provide one-button access to these features along with CallerID. Conferencing for up to 96 users is available through a Cisco Meeting Place server.

4.3.17.2 Voice Mail Services

A major component of the GRC telephone infrastructure is the CallXpress Voice Messaging System by Applied Voice & Speech Technologies, Inc. The CallXpress system, brought online in December 2008, provides voice mailboxes to all telephone system users at both the Cleveland and Plum Brook locations. In addition, the CallXpress system interfaces with the F9600 and PSTN to provide call processing. This provides special features like access to prerecorded information (e.g. inclement weather information) and the ability to access specific organizations by entering numeric information via a telephone touchpad.

4.3.17.3 E911 Services

Emergency, Fire, Medical, Safety, and Security assistance can be summoned by dialing "911" on the Center's PABX telephone system. Emergencies are defined as incidents involving serious personal injury or damage, incidents that cause possible hazardous conditions, or incidents that require immediate attention of the Plant Protection Department or Security. GRC's Emergency Dispatch Office can also be reached by dialing (216) 433-2088.

4.3.17.4 Trunks

At Lewis Field, interconnection to the public switched telephone network (PSTN) is via six (6) Integrated Services Digital Network (ISDN) Primary Rate Interfaces (PRI) lines that support both Direct Out Dialing (DOD) and Direct In Dialing (DID) calls. There is one (1) additional ISDN PRI connecting the 9600XL to the F9600ES Telephone System located at Plum Brook Station.

There are also several connections to other services. One (1) additional PRI interface with the ten (10) circuits of a T-1 are configured for DID service for DID numbers coming from the local 977 exchange. Three (3) T-1 lines connect to Federal Telecommunication System (FTS) trunks for long distance dialing. Four T-1 lines interface to the Cisco Meeting Place Teleconference server.

At Plum Brook Station, one (1) PRI provides local phone service into the Sandusky area. A dedicated ISDN Primary Rate Interface (PRI) connects the Plum Brook Station and Lewis Field telephone systems. Eight channels are utilized for communication between the sites with the remaining channels being utilized for Federal Telecommunication System (FTS) access.

4.3.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.3.19 Cable Television Services

The Lewis Information Network or LINK System (circa 1980) is a communications utility intended to provide video to the GRC community. LINK is a dual cable, bi-directional, 300 MHz CATV (Community Antenna Television) system, servicing most GRC buildings. It is capable of broadcasting on VHF Channels 2-13. The inbound capability is no longer used.

Various industry standard CATV broadband components are used in the construction of the LINK. There are both active and passive components that have 75 ohms impedance and provide 100 decibel (dB) or better shielding from radio frequency interference (RFI), electromagnetic interference (EMI) and signal ingress.

LINK backbone cable is industry standard CATV coax known as "hardline" in ½, ¾, and 1-inch sizes. This coax cable is adequate for the outside environment. It is jacketed and has a silicon, sticky, cohesive substance under the jacket to protect the coax from deteriorating from future cuts of the jacket. The coax cables are spliced in the manholes and are protected from damage from being under water.

The main service point for the LINK is Building 142, where the video distribution/control center is located and managed by the Glenn Network Operations Center (GNOC). This is also referred to as the "headend". There are three distribution legs. One serves the West Area and out to Aerospace Technology Park. The second serves the South area of campus. The third leg serves the North area of campus, including Buildings 500 and 501.

The LINK broadcasts several NASA channels, acquired from a satellite dish near Building 60 and fed to Building 142 via fiber. Additional commercial channels come from a pair of satellite dishes located at Building 142. A videoconference room in Building 3 doubles as a studio for GRC internal broadcasts (e.g. Center Director addressing the staff). The connection from this "studio" to Building 142 is via fiber.

In its present configuration, the LINK supports approximately 2300 connections. The vast majority of these connections are terminated at surface-mounted, wall plates in Center offices and conference rooms because the ports are no longer being used. Those that remain in service are typically the outbound ports connected to a variety of aging television sets.

Plum Brook Station does not feature a widespread video distribution system. Building 7141 contains access to a limited set of video services that originate at Lewis Field. A dedicated video server receives two channels from the GRC LINK system. These channels are transmitted across

the dedicated network connection between Plum Brook Station and Lewis Field. The channels are made available to a small number of office areas within Building 7141. Videoconference rooms are not available at PB.

4.3.20 Continuation of Center Zoned Architecture Project (CZAP)

The GRC NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.3.21 Ongoing Center-Specific Projects

Glenn is planning six (6) major communications projects during the NICS contract. Execution of these projects will be contingent upon receipt of funding. However, the contractor is expected to provide the design, cost estimate, and schedule for these projects so that the appropriate advocacy packages can be assembled to request funding to execute each project.

4.3.21.1 GRC Network Upgrade Completion

In the spring of 2008, GRC began implementing a multi-phase upgrade of its network infrastructure. The phases are as follows:

(I) Replace switches in key buildings

(II) Upgrade the network core to 10Gb

(III) Replace obsolete cabling and switches and provide desktop video

(IV) Align GRC with the NASA Network Consolidation Initiative

(V) Continued switch and cable refresh, augment fiber, pilot VOIP and high-speed wireless

(VI) Move video distribution to fiber, continue deploying VOIP and high-speed wireless to select areas, and continue switch and cable refresh.

Currently, only phases I and II are funded and are expected to be completed by May 2009. Funding is anticipated for Phase III, with this phase expected to start in summer 2009. Phase IV funding is dependent upon the outcome of the Agency NCI project. Execution of Phases V and VI is contingent upon available funding. Any portion of the network upgrade that is not funded and completed prior to the start of NICS will become the responsibility of the NICS contractor with details and funding to be negotiated at a later date.

4.3.21.2 GRC WAN Gateway Relocation

During the NICS contract period of performance, GRC expects to relocate the GRC WAN gateway, firewall, telephone demarcation, time code equipment, time code antenna and time code lightning protection from Building 322 to Building 142. All connections, fiber, and wiring/cabling connected to aforementioned equipment from Building 322 to Building 142 must

also be relocated with minimal disruption of service to the customer. The relocation effort will include establishing the connections necessary from Building 15 to make the WAN gateway, firewall, telephone demarcation, and time code operational. All equipment moved from Building 322 to Building 142 is to be re-synchronized and operational in Building 142 with all other NASA Center's Gateways, networks and phone systems, as well as industry/public systems currently attached to NASA GRC systems.

4.3.21.3 Telephone Service Replacement at GRC Lewis Field and Plum Brook

GRC expects to replace its telephone service at both GRC and Plum Brook during the NICS contract period of performance. The technology chosen will be based upon Agency direction matched with the infrastructure available at GRC and Plum Brook (e.g. cable plant, communications rooms, HVAC, electrical power).

4.3.21.4 GRC Video Distribution System Redesign and Replacement

During the NICS contract period of performance, GRC expects to replace its analog video distribution system at GRC with a modern fiber-based, HD digital system with desktop video capability. Extension of this system to Plum Brook may be included in the new video distribution system.

4.3.21.5 Plum Brook Station Network Redesign and Replacement

The Plum Brook network is a collection of antiquated cabling and network hubs with a scattered number of network switches. During the NICS contract period of performance, GRC anticipates a total redesign and replacement of this infrastructure.

4.3.21.6 Construction Projects

Four (4) construction projects are planned to take place during the NICS contract. Execution of these projects will be contingent upon receipt of funding. The contractor is expected to provide communications design and installation services in support of the following projects:

a) New Centralized Office Building at Lewis Field

Activities are underway to design a new Centralized Office Building which will house offices for space flight integrated project teams, a conference center, and an auditorium. Construction is planned to begin in 2010.

b) New Warehouse Complex at Lewis Field

Activities are underway to design a new warehouse complex. The complex will be located in the West Area and is intended to replace two aging warehouses.

c) New Main Gate with a shipping/receiving building at Lewis Field

Preparations are underway to construct a more secure main gate. The design includes a gatehouse and a shipping/receiving building. Construction activities are to begin in 2008 and continue through 2011.

d) New Main Entrance at Plum Brook Station

Preparations are underway to relocate the Plum Brook main entrance to a better, more secure location. Construction activities are to begin in 2008.

4.3.22 Work Load Indicators

PWS Section	Indicator	Approximate Quantities/month
3.1.1	IPAM data updates	N/A – not on IPAM yet
3.1.2	New or updated remote access accounts	5
3.1.4	Number of guest accounts	N/A – no guest accounts
3.6	Network trouble tickets	40
3.6	Network moves, adds, changes	53
3.6	Network service requests	25
3.12	IT security incident response support	15
3.12	Firewall rule changes	10
3.12	Security documentation packages	2
4.x.5	Telephone trouble tickets	50
4.x.5	Telephone moves, adds, changes	100
4.x.5	Telephone service requests	40
5.0	Network projects greater than $500K yearly	0

4.3.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.4 GODDARD SPACE FLIGHT CENTER (GSFC)

NASA's Goddard Space Flight Center is home to the nation's largest organization of combined scientists and engineers dedicated to learning and sharing their knowledge of the Earth, sun, the solar system, and universe. Goddard employees build and operate NASA science research satellites -- such as the famous Hubble Space Telescope -- manage tracking and orbital operations, and design and construct instruments flown on other NASA and international space missions.

The center's main campus is located in Greenbelt, Md., a suburb of Washington, D.C. The center is named after American rocketry pioneer Dr. Robert H. Goddard.

4.4.1 Property/Inventory

The contractor's for NISN and CNE must coordinate with the local GFSC contractor responsible for property/inventory.

4.4.2 Shipping/Receiving/Inspection

Information to be provided by Center, not yet available.

4.4.3 Vehicles Necessary To Support Center Work

Information to be provided by Center, not yet available.

4.4.4 Physical Security

Information to be provided by Center, not yet available.

4.4.5 Emergency Management

Information to be provided by Center, not yet available.

4.4.6 Safety

Information to be provided by Center, not yet available.

4.4.7 Facilities

Category/Location	Office Space	Technical Space	Lab Space	Miscellaneous Space
Building 3		4,307	1,274	1,324
Building 13		230		
Building 14 (NISN)	5,605	21,042		196
Building 25	156		1,842	

Building 28	561	2,810	532	1,953
Building 32		3,065		
Building 18	1050			
Off-Site Space	4,005			
Totals	**11,377**	**31,454**	**3,648**	**3,473**

4.4.8 Network Services

4.4.8.1 IPAM

Information to be provided by Center, not yet available.

4.4.8.2 RAS

Goddard Remote Access consists of an integrated Dial-Up and VPN approach controlled via common Security servers. The Network support group is responsible for analysis of logs, deactivation of unused accounts (after notification and warnings). Remote access capability consists of a Cisco 3030 VPN, with hardware capable of supporting 10,000 simultaneous VPN sessions, as well as 96 dial-up lines.

4.4.8.3 NTP

Information to be provided by Center, not yet available.

4.4.8.4 Guest Network

The Guest-CNE network provides a “hotel”-like wireless-only service. Users can connect unencrypted and must enter an access code, obtained from an on-Center sponsor, before gaining access to the Internet. Visitors, including personnel from other NASA Centers and approved entities, can VPN directly to their home concentrator without obtaining a guest access code.

4.4.9 Data Services

4.4.9.1 High Level LAN Description

The Center Network Environment (CNE) network provides Administrative Network capabilities via an Internet Protocol Version 4 (IPv4) Switching Infrastructure for the Goddard Space Flight Center, located at Greenbelt, MD and Wallops Island, VA. At GSFC/Greenbelt, the Network Core and Gateways to the NISN exist in Building 1 and each major building connects directly via a Gigabit Fiber Optic connection. Individual closets receive connectivity from the building switch, which is then fanned out to individual users. The type of equipment deployed is

generally Cisco Networks switches. The age of the equipment and the condition of the facilities (closet, power, HVAC, wiring) vary from location to location.

In Building 1 resides the core for the CNE network. The CNE interfaces to NISN, WAN networks, most connectivity to other GSFC Networks (HST, SEN etc.) and direct connectivity to all buildings serviced by the CNE terminate in this building. Data incoming from the WAN traverses a border gateway router, a firewall and then is distributed to the core switches. From these switches, fiber connections feed out to the remote buildings, including the "Area" distribution switch in building 201. A project to upgrade the core switches from a switched to routed environment, relocation of a core node and "dual homing" to all buildings is in work. The goal of this effort is to reduce or remove the single point of failure in Building 1.

The CNE at GSFC consists of the CNE Wired, CNE Wireless and Guest-CNE, with additional support for the FIRENet network capability at Wallops.

The high level architecture of the CNE consists of a Core, Distribution Layer (in each building) and Access Layer (to each closet). The WFF CNE is connected to the GSFC CNE via 2 MPLS paths on an OC3 circuit, with a backup circuit via a diverse route.

The CNE at GSFC supports a total of 59 buildings at Greenbelt, 35 of which are considered major (>100 drops) with a total count of 20,000 active hosts. The CNE at WFF supports 1,400 end nodes distributed over ~75 buildings; ~54 buildings on the main base, 7 on the WFF Island Mainland and 14 on the WFF Island.

4.4.9.2 Wireless Networks

Information to be provided by Center, not yet available.

4.4.9.3 Network Security

The Goddard Facilities Infrastructure Resource Environment Network (FIRENet) at Greenbelt is an air gapped stand alone network used to provide connectivity to Facility Management Division (FMD) Power and Environmental systems. This network is being expanded to include boiler control and monitoring. The network consists of 5 Cisco 3550 24 port MM fiber switches providing connectivity to individual closets. A specific Service Level Agreement (with after hours on call) has been negotiated with FMD <Do we need to include a copy here??>

The Network Group manages the Firewall providing additional protection to the Code 700 datacenter.

4.4.9.4 Network Operations

The CNE at both Greenbelt and Wallops utilizes a number of tools to monitor and manage its network infrastructure including: CiscoWorks, IP UltraMon, Wi-Spy 2.4x (For wireless), HP

OpenView, Fluke Etherscopes and SolarWinds Orion/Engineering Toolset (WFF only). There is no established and dedicated NOC for operation and management of the CNE, however establishment of such a facility is integrated into an overall network management and network operations upgrade plan, including both mission-critical and administrative networks.

The following table contains the service levels defined for CNE service, as of October 2003. (Modifications in ***italic*** are not complete)

Product/ Application	Subtask	User levels	Current Policy	Current Support	Current Service Level
IP Address management	New request			Full support	1 business day
	Move			Full support	1 business day
	Deletion			Full support	1 business day
Remote access (dial up ***and VPN***)	New accounts			Full support	2 business days
	Account deletion		Delete inactive accounts after 120 days (verification required 30 days prior to deletion)	Full support	
	Account management		Verify individuals using travel accounts every 6 months	Full support	verify individuals using travel accounts every 6 months
VPN					
Network Jacks	Activation				
	Deactivation				
Outages	GNE NW Backbone (2 or more buildings), GNE WAN/MAN Architecture, DNS, POP Server, X500, ERS	Core hours		Full support	2 hours
		non-Core hours		Full support	6 hours
	GNE NW Backbone (1 building), GNE Building Backbone, Calendar, Timeserver, IP Reg List Service, Dial-up services	Core hours		Full support	4 hours

Product/ Application	Subtask	User levels	Current Policy	Current Support	Current Service Level
		non-Core hours		Full support	4 core hours
	1 floor, Workgroup (more than 10 customers impacted by a single problem), Usenet, Network Video Services, any service not explicitly designated at another level)	Core hours		Full support	8 hours
		non-Core hours		Full support	8 core hours
	Single user	Core hours		Full support	Desktop RTS
		non-Core hours		Full support	Desktop RTS

Network Operations is responsible for the operations of the TSAN network. Network operations maintain a MAN/WAN router which provides network connectivity directly to several off-site contractors. Additional requirements may be added to the Administrative Network as a Center-wide Enterprise Architecture consolidation of external networks progresses.

4.4.9.5 Network Processes

Information to be provided by Center, not yet available.

4.4.9.6 Network Lab

Information to be provided by Center, not yet available.

4.4.9.7 Hardware Description

The CNE relies primarily on Cisco and Juniper Network Hardware. The following table identifies the types and number of Cisco switches at GSFC:

CISCO SWITCHES	
cat29408TF	1

cat295048g	1
cat297024	1
cat297024-ts	5
cat3548xl	1
cat355012g	1
cat355012t	4
cat355024	10
cat355024-mmf	1
cat355024-pwr	12
cat355048	11
cevChassisCat356024TS	2
cevChassisCat3560G24TS	1
cevChassisCat375024TS	5
cevChassisCat4006	4
cevChassisCat4503	3
cevChassisCat4506	7
wsc1900	147
wsc1900c	24
wsc2820	99
ws-c2912mf-xl	3
ws-c2916m-xl	18
ws-c2924c-xl-v	2
ws-c2924m-xl	40
ws-c2924-xl-v	123
ws-c295024	236
ws-c295024c	21
wsc4003	4
wsc5000	1
wsc5500	8
wsc5505	18
wsc5509	2
wsc6506	11
wsc6509	7
	834

The following additional hardware is deployed at the Greenbelt campus:

a. Juniper EX 4200: Qty: 151
b. Nokia Firewalls: 2 (IP 1260)
c. Juniper Firewalls: 2
d. Cisco Aironet 1100 AP's : 349

The WFF CNE consists of the following equipment:

a. Cisco Aironet 1100 AP's
b. Cisco Catalyst 4500 Modular switches
c. Cisco Catalyst 6500 Modular switches
d. Cisco Catalyst 2940/2950/2960/3550/3560 switches
e. Juniper ISG/SSG Firewalls

4.4.9.8 Hardware Refresh

Information to be provided by Center, not yet available.

4.4.10 Collaboration Services

Information to be provided by Center, not yet available.

4.4.11 Customer Relationship Management

Information to be provided by Center, not yet available.

4.4.12 IT Security

Information to be provided by Center, not yet available.

4.4.13 Cable Plant Services (RESERVED)

4.4.14 Emergency Warning Systems (RESERVED)

4.4.15 Public Address Systems (RESERVED)

4.4.16 Radio Services (RESERVED)

4.4.17 Telephone Services (RESERVED)

4.4.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.4.19 Cable Television Services (RESERVED)

4.4.20 Continuation of Center Zoned Architecture Project (CZAP)

The GSFC NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.4.21 Ongoing Center-Specific Projects

4.4.21.1 Space Science Building #34 IT Upgrade

GSFC currently has a new Space Science Building (#34) under construction at Greenbelt, scheduled for completion during 2009.

4.4.21.2 CNE IT Upgrade

Several CNE network building upgrade activities are underway at GSFC, including the design, installation and transition to a new structured cabling system and associated network electronics for the Building 7-10/15/20 complex. In addition, a network tech refresh activity is underway in Buildings 19 and 20, replacing antiquated structured cabling components, as well as network electronics. Buildings 7/10/15/29 will be completed in mid summer 2009. Base wide upgrade of out of date network electronics, facility upgrades (electrical environmental and security) continues as resources allow.

4.4.22 Work Load Indicators

Information to be provided by Center, not yet available.

4.4.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.5 NASA HEADQUARTERS (HQ)

NASA Headquarters is a single facility located at 300 E Street South West, Washington, DC. The organizations located in this facility include the Office of the Administrator, Administrator Staff Offices, Mission Directorates, and Mission Support Offices. For additional information related to NASA Headquarters please refer to www.hq.nasa.gov.

The Headquarters CIO is the Division Director of the Information Technology and Communications Division (ITCD), and is responsible for all IT programs at Headquarters. Under the leadership of the HQ CIO, the ITCD staff receives, discusses, and applies Agency and federal policy, provides principal direction and implements where appropriate within the Headquarters IT environment.

The Information Technology and Communications Division provides a full range of IT and communications services to support the programmatic and institutional functions of Headquarters employees and organizations.

The Division is also responsible for providing an effective IT management program, prescribing, developing, and implementing policies, guidelines, standards, architectures, and procedures that foster a secure, cost-effective, interoperable IT environment in direct support of NASA's mission. In conjunction with these activities, the Division assures that its services are integrated into NASA-wide services and in accordance with the Agency strategic direction.

Information and information technologies are crucial to achieving NASA's strategic goals. NASA's IT environment will need to transform to support and prepare for changes in NASA's mission activities. The NASA Chief Information Officer (CIO) has responsibility for ensuring that NASA's information assets are acquired and managed consistent with Federal policies, procedures, and legislation, and that the Agency's IRM strategy is in alignment with NASA's vision, mission, and strategic goals. To be effective, the NASA IRM Strategic plan needs to be adopted and implemented at each local center.

The HQ CIO has the responsibility for ensuring that Headquarters' information assets are acquired and managed consistent with Federal policies, procedures, and legislation, and that the HQ IT Strategic Plan aligns with the Agency's IRM strategy in support of NASA's mission. This document is a companion plan to the NASA IRM Strategic Plan and is meant to demonstrate how the broader goals of that plan can be applied within the Headquarters IT environment and Enterprise Architecture.

4.5.1 Property/Inventory

Information to be provided by Center, not yet available.

4.5.2 Shipping/Receiving/Inspection

Information to be provided by Center, not yet available.

4.5.3 Vehicles Necessary To Support Center Work

Information to be provided by Center, not yet available.

4.5.4 Physical Security

Information to be provided by Center, not yet available.

4.5.5 Emergency Management

Information to be provided by Center, not yet available.

4.5.6 Safety

Information to be provided by Center, not yet available.

4.5.7 Facilities

The Headquarters facility has nine (9) floors and concourse level that are fully occupied by approximately 1670 NASA civil servant, and contractor personnel. The staff located at Headquarters, are distributed across each of the nine (9) floors of the building. The concourse level provides office space for contractor support personnel, the HQ Data Center, NISN Gateway, NASA TV, and Video Conferencing facilities.

The Headquarters facility was constructed and first occupied by NASA in 1992. There have been no substantial modifications to the facility since construction, or initial occupancy. The infrastructure support systems and services have been fully maintained and updated as necessary. These updates and maintenance activities include the replacement of all communication room air conditioning units in 2007, installation of a Cat5e LAN cable plant to all offices. In addition the Headquarters data center was updated with new server racks, power distribution, and cable plant in 2008. The facility is also equipped with a data center class UPS system that is capable of providing filtered power to the data center, and all communications closets. With the installation of the backup emergency generators in 2006, electrical power can be maintained for extended periods of time.

The space occupied by HQ IT support personnel whose functions will transition to NICS is as follows. The space identified is located within the Headquarters building. The contractor staff supporting HQ has access to, and may schedule meetings in any of the facilities conference rooms.

Short term requirements for storage can be arranged through the HQ Facilities organization. No long term storage is provided.

Type of Space	SQUARE FOOTAGE
Office Space/NOC/NISN Gateway	1850
Technical Space	
Storage	As needed
Lab	
Conference Room	
Miscellaneous	

4.5.8 Network Services

4.5.8.1 IPAM

Information to be provided by Center, not yet available.

4.5.8.2 RAS

Headquarters provides three types of remote access services, each designed to meet specific customer need, or IT security requirements. These services include a traditional IP Sec VPN, SSL VPN, and low speed dial in service. The IP Sec VPN solution requires preconfigured client software that has been included in the Headquarters ODIN core software load on all PC and Mac laptops. A requirement for use of the IPSec VPN service is an ODIN provided and maintained laptop. This solution consists of a Cisco 3080 VPN cluster in a high availability configuration. In addition to the IPSec VPN service, Headquarters also provides an SSL VPN service. This service was deployed to provide remote access to workstations that are not provisioned or maintained by the ODIN vendor. The SSL VPN solution consists of a pair of Juniper AS4000 appliances in a high availability configuration. The AS4000s are licensed for 500 concurrent users. The legacy low speed (56Kbs) dial in service is maintained to support the access requirements of Headquarters personnel that do not have high speed access from the location they may be at. It is the intension of Headquarters to decommission this low speed service no later than FY10.

4.5.8.3 NTP

Information to be provided by Center, not yet available.

4.5.8.4 Guest Network

Information to be provided by Center, not yet available.

4.5.9 Data Services

4.5.9.1 High Level LAN Description

The base Headquarters network architecture was developed and implemented in 1998, and has proven to be flexible, adaptable, and scalable. Although all components of the system have been replaced multiple times through their lifecycle, the underlying architecture has not been required to change or undergo substantial modifications.

The Headquarters local area network provides 100/1000Mbs connectivity to all workstations and servers that reside at this facility. There is a single local area network with multiple security boundaries. The policies associated with these boundaries are enforced by the core and project level firewalls. The firewall policies are tailored to the service requirements of the devices that reside on these network segments.

The layout of the facility requires the use of three communications closets per floor. Each communications closet is provisioned with a primary and backup communications path. The center communications closets on each floor provide the primary path to each east and west wing communications closets. The backup communication path for each east and west wing closet is provisioned through a redundant path to the floor immediately above or below. The primary communication path from each floor is a direct connection to the Headquarters Computer Center (NHCC). The backup path from each floor is provisioned through the Concourse Center communication closet. To support the communication requirements of the facility, Headquarters utilizes a multi-mode fiber cable plant. The communication trunks from the east and west communications closets to the center communications closet on each floor are 1000Mbs. The communication trunks from each floor center communications closet to the NHCC or Concourse Center is 2000Mbs. In the first quarter of calendar your 2009 the HQ LAN upgrade project will move to the implementation phase. This project will upgrade all network trunks to 10G. The hardware required to complete this activity has been procured and is to be fully installed by July 2009.

The Headquarters LAN network components are exclusively Cisco Systems equipment, specifically the Catalyst 6500 LAN switch. Currently, the primary supervisor module deployed at the access layer is the Sup2, with a Catalyst OS. After the completion of the current upgrade initiative, the east and west floor closet switches will utilize the Sup32 with native IOS. All floor Center communications closet switches and distribution layer/Core will utilize the Sup720 with native IOS. The remainder of this section describes the to-be state after the upgrade project has been completed. The switches at the access layer are the Catalyst 6506e in each of the east and west wing communications closet. The switches in each floor center communication closet are the Catalyst 6509e. The NHCC combined core and distribution layer utilize a redundant pair of Catalyst 6509e switches in a High Availability configuration. The line cards utilizes with the 6500 chassis are a combination of supervisor 720, supervisor 32, 10G blades, and 10/100/1000Mbs line cards with Power over Ethernet (PoE).

4.5.9.2 Wireless Networks

The Headquarters wireless network provides Private Network, and Guest Network services to all areas within the facility. To provision this service, 128 Cisco AP1200s have been deployed throughout the building. The Guest network utilizes a Blue Socket 2200 captive portal appliance. The private Network wireless requires encryption and two factor hardware token authentication for access. All systems associated with the Headquarters wireless network service are current and of vendor supportable hardware and software. Recent enhancements include the replacement of the Blue Socket captive portal to allow the Headquarters Guest network to scale to 400 concurrent users.

4.5.9.3 Network Security

The firewalls utilized by Headquarters are exclusively CheckPoint NGX appliances. The firewalls protecting, or isolating critical services are in a High Availability configuration. These firewalls include the Core, Services (remote access and wireless), contractor, and Network Operations Center. Less critical firewalls are in a single appliance deployment configuration. These firewalls include the Guest network, and the Systems Engineering Facility (SEF) test lab. All firewall enforcement engines are managed through a High Availability management cluster by the HQ NOC. The policies, or rule sets applied to these firewall vary depending on the resources they are protecting. The Core firewall that protects the Headquarters Private network and the HQ Guest Network have a base policy of default deny inbound and default allow outbound. All other firewalls, and firewall protected networks have a default deny inbound and default deny outbound.

4.5.9.4 Network Operations

The Network Operations Center (NOC) is located in a controlled access adjacent to the Headquarters Data Center. The NOC, as with the entire HQ Operations Team, is staffed from 6am to 6pm Monday-Friday. After hours and weekend support is provided on an as scheduled and failure response basis. The primary function of the HQ NOC is the management, maintenance, enhancement to, and monitoring of all aspects of Headquarters network services. The support provided by the NOC not only include Headquarters based services, but those services accessed by customers that are external to Headquarters. This support includes the coordination of troubleshooting with counterparts at the NASA Field Centers, Agency partners, and external entities. As part of the daily activities, the HQ NOC supports the move/add/change requirements of the facility. Part of this activity includes the setup and disabling of network LAN switch ports. The NOC has established processes and procedures to accomplish these activities that include standards for the switch port description field, proper QoS settings, and ensuring that all unused ports are in a disabled state.

The Headquarters NOC is responsible for the maintenance, management, enhancements to, and monitoring of all Headquarters firewalls. The NOC provides firewall rule set and router ACL analysis and modification to support the deployment of new services at Headquarters. In addition, the NOC also reviews and recommends actions necessary to implement IT Security recommended system and service blocks for hostile, or out of profile communication flows.

Unlike a traditional NOC, the HQ NOC is a hybrid that includes both operations and engineering functions. In a traditional Engineering and Operations environment, the Engineering department is responsible for the development of system and service enhancements. The project is then transitioned to the Operations organization for implementation and sustainment. At Headquarters these functions have been consolidated into the NOC. When necessary, Systems Engineering department resources are available, and applied. The monitoring and management tools utilized by the Headquarters NOC are HP OpenView, CiscoWorks, MRTG, and Nagios. The NOC provides monitoring and automated alerting services for all network systems, network components, and HQ based servers and services. The monitoring, and alerting is not limited to base level ICMP up/down, the NOC also monitors the services and health and condition of all devices. When predefined thresholds are exceeded, alerts are sent to the proper support personnel. This proactive approach to service and systems monitoring allows support personnel, in almost all cases to resolve an issue prior to a service outage and customer impact. The availability metric for Headquarters networks and services consistently achieve 99.999%.

4.5.9.5 Network Processes

Information to be provided by Center, not yet available.

4.5.9.6 Network Lab

Information to be provided by Center, not yet available.

4.5.9.7 Hardware Description

Information to be provided by Center, not yet available.

4.5.9.8 Hardware Refresh

Headquarters has established a lease contract for the major components that make up the LAN. This enables HQ to maintain the currency of all network systems, and maintain high levels of service availability. The baseline network switch at Headquarters is the Cisco Catalyst 6500. The devices currently in production were deployed in 2004 and are scheduled to be replaced in 2009 through the renewal of the HQ Lease contract. The term of this lease contract is a period of four years that will expire in 2012. It is anticipated that the replacement for the Catalyst 6500 platform will be available at that time, and a follow on lease contract will be established for the life cycle replacement of the Headquarters LAN.

The life cycle replacement of all other Headquarters network systems and services are defined initiatives within the Headquarters Tactical Plan.

4.5.10 Colloaboration Services

Information to be provided by Center, not yet available.

4.5.11 Customer Relationship Management

Information to be provided by Center, not yet available.

4.5.12 IT Security

Information to be provided by Center, not yet available.

4.5.13 Cable Plant Services

The cable plant that services all end user locations within the facility is comprised of dual Cat5e runs (data 1 and data 2) to each office within the building. The cable runs terminate into industry standard patch panels located in the closest communications closet (floor east-center-west). To support the as necessary movement of office cubicles, or office walls, the entire facility has a raised floor structure. This six inch raised floor permits the movement of network drops, or installation of additional drops anywhere in the facility without the need for extensive work or facility modifications.

The facility is also equipped with a 62.5 micron multi mode fiber cable plant. Each wing communications closer (east and west) has fiber runs installed to the center communications closet on that floor. In addition fiber runs have been installed to the wing closet immediately above or below. The center communications closet on each floor is home run to the Concourse center communications closet, and the HQ Data Center. All fiber cables terminate into industry standard patch panels. In all communications closets and the Data Center, there is excess fiber cable capacity to support future requirements or needs.

The Headquarters Telecommunications team is responsible for patching and proper labeling of all cables, both cupper and fiber, as directed by the HQ NOC. All cables are required to be labeled on both ends, and properly laced into cable trays and runs.

4.5.14 Emergency Warning System

See information in section 4.5.15 of this document.

4.5.15 Public Address System

The Telecommunications team is responsible for the installation and maintenance of the Headquarters Valcom Public Address (PA) system. The system is in a loop configuration, 24VDC Tip and Ring. There are approximately 1000 speakers thought the facility that provide announcement capability to all areas of the building to include office space, restrooms, stairwells, parking garage, and all common areas such as the auditorium, and conference rooms. The broadcast capabilities are provided through Valcom microphones that are strategically located in the Space Operations Center, Main Physical Security office, and the Emergency

Operations Center. The Telecommunications team maintains this PA system, effects repairs, and relocates speakers as necessary to support facility alterations.

4.5.16 Radio Services (RESERVED)

4.5.17 Telephone Services (RESERVED)

All HQ Centrex, and analog line services should be fully phased out or converted to VoIP by the end of FY09. No support requirements are anticipated for non-VoIP related telephone services.

4.5.18 Voice over Internet Protocol (VoIP)

The Headquarters voice communication service is provisioned through a Cisco Voice over IP system. The services provisioned include local, long distance, international calling, and voice mail services. All elements of this critical service are configured for high availability with no tolerance for service interruption. The Cisco 7970 telephone desk sets are powered through the use of Power over Ethernet (PoE) from the communications closet network switch. The switches are serviced by the facility UPS and backup power generators to ensure telephone services remain operational in the event of a facility poser outage. To ensure all modifications, enhancements, and changes to this system are fully tested a substantial investment has been made to duplicate all critical elements of this system in a lab environment. The VoIP system deployed at Headquarters consists of a Cisco Call Manager publisher, multiple subscribers (4 MCS-7845), Unity voice mail, and multiple gateways (6 CS2801) with 10 PRIs. The service is scaled to exceed the service requirements of the Headquarters customer community. The recent projects associated with the VoIP service include the migration to a LINUX based appliance operating system, and substantial enhancements to the system and service monitoring system. The Headquarters telecommunication team has implemented the CaseSentry monitoring tool that was designed to provide enhanced monitoring and reporting capabilities of a Cisco based VoIP solution.

The planned activities associated with the HQ VoIP system are both internally and externally facing. The internal facing elements are focused on system and service enhancements that include soft phone technology, and E911 services. These activities are currently in work and scheduled to be completed in FY09.

The externally facing enhancements will be ongoing activities. These include the design and implementation of an automated failover capability to an alternate location, and the ability to route calls to other NASA VoIP systems over the NISN WAN. Headquarters, DFRC, and NISN have established this capability between lab environments. As the design fully matures it will be implemented across all VoIP participating Centers.

4.5.19 Cable Television Services

The Telecommunications team has limited responsibilities associated with the Cable, and Satellite TV services provisioned at Headquarters. The Cable TV service is provisioned through Washington Cable. The Cable TV vendor maintains responsibility for the proper operation of the equipment used to support this service. When problems arise with the cable TV equipment, the Headquarters Telecommunications team is responsible for coordinating the vendor repair of the faulty equipment. The same relationship is in place for the 5 locations that receive the high definition Satellite TV service. The primary responsibility of the Telecommunications team is to patch customer office locations into the Cable TV service. The TV cable plant distribution is very similar to the LAN cable plant. The Cable TV connection point for an office is the nearest communications closet to the customer location.

4.5.20 Continuation of Center Zoned Architecture Project (CZAP)

The HQ NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.5.21 Ongoing Center-Specific Projects

Information to be provided by Center, not yet available.

4.5.22 Workload Indicators

Information to be provided by Center, not yet available.

4.5.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.6 JET PROPULSION LABORATORY (JPL) (RESERVED)

4.7 JOHNSON SPACE FLIGHT CENTER (JSC)

Johnson Space Center was established in 1961 as the Manned Spacecraft Center. In 1973, it was renamed in honor of the late President and Texas native, Lyndon B. Johnson. From the early Gemini, Apollo and Skylab projects to today's space shuttle, International Space Station and Exploration Programs, the center continues to lead NASA's efforts in human space exploration. The JSC civil service workforce consists of about 3,000 employees, the majority of whom are professional engineers and scientists. Of these, approximately 110 are astronauts. About 50 companies provide contractor personnel to JSC and more than 12,000 contractors work onsite or in nearby office buildings.

JSC is home to NASA's astronaut corp. The center is responsible for the training of space explorers from the United States and our space station partner nations. As such, it is the principal training site for both space shuttle crews and International Space Station Expedition crews.

The center's famed Mission Control Center, or MCC, is often referred to as the nerve center for America's human space flight program. Since 1965 and the Gemini IV era, men and women who work in MCC have been instrumental to the success of every crewed spaceflight. Today the MCC supports all space shuttle and station missions and simulations. JSC has a team of dedicated professionals who manage the development, testing, production and delivery of all U.S. human spacecraft, and all human spacecraft-related functions.

JSC associated component facilities include: Ellington Field, Sonny Carter Training Facility, and the White Sands Test Facility, which includes the El Paso Hanger. A brief description of the component facilities is as follows:

a) Ellington Field

Ellington Field is the heart of Johnson Space Center's flying operations. NASA's primary function at Ellington is the training of astronauts for spaceflight. The field is also a base for administrative, cargo transport and high-altitude aircraft, with many types of NASA aircraft at the hangers.

b) Sonny Carter Training Facility: The Neutral Buoyancy Laboratory

The Neutral Buoyancy Laboratory (NBL) was named after Astronaut Manley L. "Sonny" Carter, Jr. The mission of the NBL is to prepare for space missions involving spacewalks. NASA team members use the NBL to develop flight procedures, verify hardware compatibility, train astronauts and refine spacewalk procedures during flight that are necessary to ensure mission success.

c) White Sands Test Facility

WSTF is located on a 64,000 acre campus near Las Cruces, New Mexico. The facility location was selected in 1962 by NASA Headquarters and was known as the Apollo site until 1965. In 1964, the first rocket engine was test fired. Since then, the test facility has supported the Apollo, Viking Lander, Cassini, Space Shuttle, International Space Station and other NASA programs. White Sands Space Harbor, operated by White Sands, supports astronaut space shuttle training and is the alternate landing site for both Kennedy Space Center and Edwards Air Force Base. WSTF is a tenant of the White Sands Missile Range (WSMR) (DOD, Army).

A self-contained facility with medical, fire and hazardous rescue personnel, White Sands Test Facility supports other governmental agencies, including the Department of Defense, the U.S. Navy and the U.S. Air Force, with materials and propulsion testing. The test facility conducts training on hazardous fuels throughout the U.S. and abroad and also produces technical papers and reports. Testing of Materials for NASA has been conducted at WSTF since the Apollo Program. The mission of WSTF is to be the preeminent resource for testing and evaluating potentially hazardous materials, spaceflight components, and rocket propulsion systems. Its objectives are to return the space shuttle to flight, help complete the assembly of the International Space Station, develop the Crew Exploration Vehicle, return humans to the moon, and pursue human exploration of Mars and the solar system. We are accomplishing this mission as well as inspiring the next generation of explorers with an active educational outreach program.

The White Sands Space Harbor (WSSH) is a tenant of WSMR and is approximately a one hour drive from WSTF main campus. WSSH operates daily with ongoing operations that support the STA training aircraft as well as supporting every Shuttle launch and landing. IT support could be Mission critical if the Shuttle were to land at WSSH.

There are about 700 onsite civil servants and contractors working at WSTF, including WSSH and the El Paso Hanger.

d) El Paso Hanger

Located in El Paso, TX, the El Paso Hanger Operations is a tenant of the El Paso International Airport and is approximately a one hour drive from WSTF main campus. The El Paso Hanger supports astronaut flight training, among other activities.

Note: White Sands Complex (WSC) is not affiliated with the Johnson Space Center, rather it belongs to Goddard Space Flight Center. WSC is 3 miles north of WSTF.

The current service delivery approach for IT services at JSC and WSTF is a combination of the ODIN, JETS, JIMMS, & NISN contracts.

4.7.1 Property/Inventory

Under the current service delivery model, JSC IT contractors work with Center Operations Director property management group. The contractor performs property management and administration of all property acquired by, or in possession of, the contractor and subcontractors including both Government Furnished Property and Installation Provided Equipment. RFP Attachments J-8, *Government Furnished Property*, and J-9, *Installation Accountable Government Property* delineates the list of equipment that will be managed by NICS.

4.7.2 Shipping/Receiving/Inspection

The NICS contractor will work with the Center Operations Directorate for shipping and receiving at JSC. The contractor may utilize the Center's shipping and receiving facility but is not required to do so.

All deliveries of inbound freight at JSC (FedEx, UPS, Yellow Freight, Consolidated Freight, vendors, etc.) for either civil servants or contractors must be received and security screened at Building 421, Central Receiving.

All inbound NASA JSC shipments should be addressed as follows:

NASA-JSC Transportation Officer
Attn: Name, Phone No.
Building 421
2101 NASA Parkway
Houston, TX 77058
Hours: 7:30 a.m. - 3:30 p.m. M-F

All on-site outbound shipments must be picked up by carriers at Building 420, Packing & Shipping. The contractor must ensure appropriate protection of the shipment during handling and transport. Shipments must be packed, marked, and labeled before pick-up by the carrier. When making outbound shipments from JSC, you may either schedule your shipments to be picked up from your location or you may drop off your shipments at Building 420. All deliveries are between 7:30 a.m. and 3:30 p.m., Monday-Friday, excluding holidays. Carriers may enter the Center only if prior coordination has taken place.

4.7.3 Vehicles Necessary To Support Center Work

At least one truck or van will be required for implementing the local area networking requirements for the JSC campus in Houston, TX. White Sands Test Facility in Las Cruces, NM will also require at least one truck or van.

4.7.4 Physical Security

The NICS contractor will work with the JSC Center Operations Directorate (COD) for physical security controls. Facilities at JSC have a variety of physical access controls, including keys for wiring closets, cipher-lock codes for certain closets and rooms, and badge reader access for critical areas of the campus, such as the mission control center facility and the data center.

4.7.5 Emergency Management

The NICS contractor will work with the JSC Center Operations Directorate's Emergency Operations Center (EOC). The EOC is provided the information regarding telephone number to location mapping for emergency calls. The NICS contractor will support the Center's COOP plan.

4.7.6 Safety

Hazardous test facilities require specific safety plans to handle support in hazardous environment.

JSC and WSTF each have facilities that contain asbestos, particularly in ceiling tiles and the adhesives used for ceiling tiles. Work performed in facilities that require disturbing asbestos must be conducted using the proper safeguards by personnel who are trained to deal with asbestos. The contractor must adhere to the JSC Safety and Health plan.

4.7.7 Facilities

The JSC main campus is comprised of 168 buildings, of which 144 have network/telephone infrastructure. Ellington Field is located about 15 minutes north of the main JSC campus, and is comprised of 29 separate buildings, of which 14 have network/telephone infrastructure. The SCTF is also located about 15 minutes north of the main JSC campus, and contains three buildings with network/telephone infrastructure. WSTF has 48 buildings, 8 of which are located at the WSSH. The El Paso Hanger contains two buildings.

At WSTF, the administrative buildings are located in the 100 Area, Hazardous testing and associated buildings are the following:

a) Laboratories and Hypervelocity are located in the 200 area.
b) Propulsion Test stand operations are located in the 300 and 400 areas.

c) Impact Testing in the 500 area

Every facility at JSC has at least one wiring closet, which is the location where the network and telephone equipment has been installed. Because most of our facilities are fairly old, the data and telephone networks have been squeezed into places that are not optimal and in some cases harmful to our equipment. IRD has a multi-year project to refurbish our wiring closets to better prepare for future network requirements, including utilizing the data network for more voice and video applications. There are a total of 386 in JSC main campus facilities.

Facility Space for NICS personnel after contract start:

a) B46 Network Operations Center ~ 1452 sq ft
b) B46/200 (current JETS Firewall operations) ~ 1152 sq ft
c) B17/134 (JSC main campus telephone equipment) ~ 1500 sq ft
d) B17/142 (Telephone engineers and operations) ~ 300 sq ft
e) B32 (Campus backbone equipment room) ~ 300 sq ft
f) On-site Storage ~ 2000 sq ft in B46 (shared storage space)

Note: ODIN contractor has leased an off-site building to support JSC that has space for both their personnel not located onsite and warehousing of equipment.

Category/Location	Office Space (sq ft)	Technical Space (sq ft)	Lab Space (sq ft)	Miscellaneous Space (sq ft)
Building 46 Network Operations Center	1452			
Building 46 Room 200	1152			
Building 46				2000 (shared storage)
Building 17 Room 134		1500		
Building 17 Room 142	300			
Building 32		300		
Off-Site Space	30,200			
Totals	**11,377**	**31,454**		

4.7.8 Network Services

JSC has infrastructure described below that support network services including IPAM, RAS, NTP, and Guest Network.

4.7.8.1 IPAM

The IPAM appliances will provide DNS and DHCP for clients. The NICS contractor will be responsible for three agency IPAM appliances at JSC. Two of these servers reside on the internal network and one resides on the JSC ISOLAN. WSTF will have one agency IPAM appliance, which will be backed up by the IPAM appliances at JSC. The NICS contractor will sustain the IPAM appliances and manage the information contained in the IPAM database.

4.7.8.2 Remote Access Services (RAS)

JSC offers several remote access solutions for its employees, including dial up networking, a Juniper SSL VPN, and a legacy VPN using Microsoft PPTP. JSC remote access solutions require two factor authentication (domain accounts with RSA token) to access.

Remote Access Hardware:

a) Two Dell PE 2950 (JSC PPTP)
b) Four Juniper SA 6000 (JSC Juniper SSL VPN)
c) Two Dell PE 2950 (WSTF Radius Server, PPTP)
d) Two Juniper SA 4000 FIPS (WSTF Juniper SSL VPN)

At JSC, the number of users with approved remote access using RSA Secure ID tokens is approximately 6500. At WSTF, the number of users with approved remote access using RSA Secure ID tokens is 280.

4.7.8.3 NTP

JSC has two Cisco routers that are serving as NTP servers for the local area network on the main campus at JSC. All network devices that will be managed by the NICS contractor at JSC point to those two NTP sources, which point to NISN's Stratum 1 clock, currently managed by the UNITeS contract.

4.7.8.4 Guest Network

The JSC Guest Network is a partition of the JSC network that allows official guests to make limited use of government IT resources, including but not limited to: Internet connectivity, access to Internet services, VPN, and e-mail for NASA-related business use. The JSC Guest Network is available 24 hours a day, 7 days a week. The guest network currently has a registration process that requires a NASA sponsor to request a user ID and password for their guest. JSC is moving toward a self-registration model that is expected to be in place by the beginning of the NICS contract.

The JSC Guest Network features both wireless and wired connectivity options (wired currently limited to specifically designated areas). All wireless network access points are configured to allow access to the Guest Network. The WSTF Guest Network follows the JSC model, but is only available via the WSTF wireless network.

4.7.9 Data Services

4.7.9.1 High Level LAN Description

The JSC network is mainly comprised of Cisco Systems hardware. The local area network (LAN) follows a three-tiered hierarchical model, with core, distribution and access layer devices.

The access layer switches are mostly Cisco IOS based 10/100 Mbps switches with Power over Ethernet (PoE) and Gigabit Ethernet uplinks to redundant distribution devices. There are approximately 600 access layer switches on the JSC network, most of which are Cisco Catalyst 3560 48 ports 10/100 Mbps switches. Some portions of the network have 10/100/1000 Mbps connections, mainly for the server infrastructure and some labs that have high speed network requirements.

Most of the distribution devices are Cisco Catalyst 6506E switch/routers. The distribution layer redundancy effort was begun in FY 2007 and is scheduled to be completed in FY 2010. Each distribution layer device is redundantly connected to two core layer Cisco Catalyst 6500 switch/routers. Routing is accomplished via OSPF protocol, with some EIGRP for connections to network devices managed by other contractors or organizations.

Other important network technologies used on the JSC LAN include extensive use of VLAN (sub-networks of a Class B address space), Quality of Service, multicast, and voice and video over IP.

JSC's connection to the wide-area network is provided via the UNITeS contract's NISN network. JSC has redundant connections to the SIP network and the PIP network, NISN terms for wide-area networks managed by the UNITeS contractor.

There are approximately 20,000 network drops across the JSC campus and associated facilities, not including WSTF.

WSTF follows the same architecture and high level design as JSC facilities, including use of the same hardware models for access and distribution layers. There are several circuits provided by NISN to the WSTF and associated facilities:

a) OC-12 connectivity to JSC

b) Redundant connectivity to NISN backbone through Dallas CIEF
c) DS-3 connectivity to El Paso hanger
d) DS-3 connectivity to WSMR with tails supporting Orion Project to L- Complex 32 and a separate tail circuit to WSSH.

There are approximately 700 active network drops on the WSTF LAN. The WSTF standard office has two network connections and one phone connection per drop. Each office on site has at a minimum one drop. There are approximately 1000 network drops on site.

4.7.9.2 Wireless Networks

The JSC Wireless network is a separated logically and physically from the center's private LAN by a firewall. Most communications are unrestricted, however, between the wireless LAN and the private LAN.

The wireless network is comprised of Aruba centralized controllers with Aruba Access Points. There are approximately 250 access points (Aruba 61) that are installed throughout the center. There are approximately 40 access points at WSTF. Access points have been growing at a rate of over 50 per year for the past several years. The wireless network also includes wireless intrusion detection sensors (Aruba 65). Access to the wireless network is provided by the PEAP protocol, and AES encryption is used to secure the data transmitted via wireless.

The JSC wireless network access points all provide both the limited access wireless network for employees of JSC as well as the Guest Network.

4.7.9.3 Network Security

JSC and WSTF have extensive firewall systems that protect the networks in a layered approach. The current configuration is expected to change with respect to the Center Zoned Architecture project. Currently, JSC uses four Juniper NS-5200 Firewalls as the main protective barriers for the center, which forms two security zones. The outer zone is called the ISOLAN, which is where JSC contractors and some public facing services reside. The inner zone is the center's private network. There are also smaller subdivided security zones created by the DMZ firewalls, which are Juniper ISG 2000 appliances.

WSTF has a set of Juniper firewalls to protect their campus during times when the main network link connecting the WSTF and JSC private LANs is disabled (such as during hurricane Ike in 2008) and WSTF has its own interface to the WAN activated.

On the ISOLAN, there are twelve sets of Cisco 1410 wireless bridges that connect metro area contractor facilities to the JSC network. These facilities currently include Indyne, Jacobs

Sverdrup, Draper Labs, Wyle, Hamilton Sundstrand, GB Tech, USA, Bastion, Blackhawk, Barrios and Oceaneering. Some locations require additional bandwidth and are connected to JSC via leased circuits. These locations currently include the Boeing, USA, and SAIC facilities.

As part of the managing the center's private network, there are areas of the campus that contain networks managed by other entities. Examples include laboratory environments and Mission support areas, such as simulator and training environments. Connectivity for these networks must be coordinated by the NICS contractor.

To further protect the center's private network, JSC uses two Bluecoat SG8100 devices as proxies for outbound web traffic.

4.7.9.4 Network Operations

The Network Operations Center (NOC) at JSC is located in the JSC Data Center, and it acts as the central monitoring and management facility for the entire JSC data network. This facility is staffed by ODIN network administrators 24 hours a day, 7 days a week. ODIN network administrators in the NOC remotely manage all the network devices on the JSC institutional data network, which includes all JSC associated component facilities. They also have access to all the data collected by network monitoring tools, displayed on four high definition large screen monitors.

CiscoWorks LAN Management Solution (LMS) is used to remotely manage the network infrastructure from the Network Operations Center (NOC) in Building 46.

Other Network Monitoring applications (managed by either ODIN or JETS):

a. Niksun NetVCR - This is a network performance and analysis tool that captures, stores, and analyzes complete network traffic data. IRD currently uses two units, one that collects data from the JSC internal network and one that collects data from the isolation network that allows our off campus local area contractor community to communicate with the JSC network.
b. Orion Solarwinds - Network performance monitoring tool. Using the simple network management protocol (SNMP), various conditions of network devices and alerts the IRD network engineering team when network devices are struggling to transmit data throughout the network. This tool is used to assess traffic loads on various network links, and it provides a graphical representation of the amount of data traversing the JSC network.
c. Out of Band Monitoring Network (Traffic Sniffing) - This network is a separate network from that regular data network that is designed to allow network traffic to be copied to monitoring devices that can analyze the traffic for the purposes of troubleshooting issues on the network. This "on demand" traffic capturing capability is currently connected to

most building routers on the JSC internal network. The system gives the network and IT security team the capability of remotely capturing data for troubleshooting, which significantly reduces troubleshooting response time.

d. Cisco Unified Operations Manager - This tool provides real-time, monitoring of all elements or our limited VoIP deployment. It performs automatic discovery for the entire system and provides contextual diagnostics for rapid troubleshooting.
e. Cisco Unified Service Statistics Manager - Monitoring tool that collects and analyzes statistics from a variety of sources to define service-level agreement (SLA) for our Voice over IP (VoIP) deployment.
f. IPERF - IPERF is an open source network troubleshooting tool used to measure bandwidth capacity between two points on the network. It is often used by the network team to verify that expected bandwidth is being achieved by the network.
g. Nagios - Free open source tool that monitors current network and server status for availability. This tool is an alternative to Solarwinds.
h. Multi Router Traffic Grapher (MRTG) - Free open source tool to monitor traffic load on network links. This tool is an alternative to Solarwinds.
i. HP OpenView - ODIN uses HP OpenView (HPOV) in the Network Operations Control Center to monitor up/down status of all ODIN-managed network devices. HPOV logs information from network devices.
j. APC UPS Monitor – ODIN uses this system to monitor the condition of uninterruptible power supplies.

4.7.9.5 Network Processes

JSC and WSTF customers use the Customer Service System, a website service ordering system, to purchase services from the current service delivery contracts. The Center has a Network Access Control Board (NACB) that approves network and firewall changes with IT security requirements, chaired by the Information Resources Directorate (IRD). The NACB is supported by both civil servants and the JETS contract. Major network architecture changes are approved by the IRD Control Board (ICB), which is chaired by the JSC CIO.

4.7.9.6 Network Lab

JSC CIO has a lab in Building 46 that contains a sampling of network hardware similar to that used in the JSC campus. There are routers, switches, firewalls, wireless, VoIP equipment, and other assorted network components that can be used by contractors or civil servants in assessing, evaluating, testing new technology, changes in existing infrastructure, and upgrades.

4.7.9.7 Hardware Description

Included in previous sections.

4.7.9.8 Hardware Refresh

JSC has a network obsolescence plan that is maintained to replace equipment on a scheduled basis, with a base lifetime for each piece of network hardware set at five years.

4.7.10 Collaboration Services

4.7.10.1 JSC Video Teleconference Rooms

All video teleconference scheduling and room booking at JSC is done through the JSC Video Teleconference (JSC ViTS) Coordinator at 34755. Video Teleconferences are booked on a first come, first served basis. Video Teleconferences are to be scheduled at least three days in advance for NASA connected meetings. Other connections may require considerably more advance notice. If you are booking a video teleconference, call the JSC ViTS Coordinator with the desired date(s), time(s), station locations and contact name for each station. The JSC ViTS Coordinator will verify system and station location availability to book that time or work out acceptable alternatives. If you are notified that you are to be included in a video teleconference at JSC, call the JSC ViTS Coordinator to determine what JSC ViTS room your meeting is scheduled for and/or to discuss any questions regarding the meeting. The rooms are described below:

Building	Room	Seating Capacity	Note
1	360A	72	
1	457A	46	
1	818	25	
4S	4519	65	Space Station Only
8	2100	21	
17	2026	28	
30S	2312	49	requires CAA access

WSTF has 3 primary ViTS rooms as described below:

a) One large room, Rotunda (Auditorium) serving a capacity of 175 employees
b) One medium room, B101 ViTS room serving 25 employees
c) One small room serving 12 employees.

4.7.11 Customer Relationship Management

The JSC CIO is organized to provide a Customer Relationship Manager for each organization at JSC. The following tables show network demarcation points and customer interface points for local area networks at the Center not managed by the CIO, to include external, perimeter, near-site, off-site and internal touch points.

External/Perimeter/Off-Site/Near-Site

Interface Name	Supporting Organization	Description
United Space Alliance (USA) network	United Space Alliance (USA)	The USA network interfaces with the JSC network through a direct link to JSC's border routers. USA has a NASA provided AT&T Gigaman circuit and a redundant connection through a Cisco Wireless Link. USA offices are located at 600 Gemini St. Houston
European Space Agency (ESA) interface	ESA	ESA interfaces with JSC through a direct link to the JSC DMZ network.
Italian Space Agency (ASI)	ASI	ASI interfaces with JSC through the JSC DMZ network.
SAIC Network	NASA IRD	IRD-ODIN maintained network located at 2450 NASA Parkway.
Boeing Network	Boeing	The Boeing network interfaces with the JSC network through the ISOLAN. The network is located in 13100 Space Center Blvd. Boeing is a separate VLAN on the AT&T Gigaman circuit that connects SCTF to JSC.
Space Center Houston	NASA IRD	SCH connects to JSC using NASA owned copper infrastructure (a T-1 like connection) and the demark point is the ISOLAN.
SPACE HAB	SPACE HAB	Non IRD maintained network that uses JSC assigned IP address space.
Lockheed Martin Information Technology (LMIT)	LMIT	Non IRD maintained network located in 555 Forge River Rd. Connects to JSC using a Phonoscope circuit and the demark point is the ISOLAN.
ARES	ARES	The Ares network interfaces with JSC through NASA provided Cisco wireless bridges between the Armand Plaza A Bldg located in Space Center Blvd. and 2525 Bay Area Blvd. At 2525 Bay Area a Gigaman circuit is used to connect Ares and other contractors back to the ISOLAN.
BARRIOS	Barrios	The Barrios network interfaces with JSC through NASA provided Cisco wireless bridges between the Armand Plaza B Bldg located in Space Center Blvd. and 2525 Bay Area Blvd. At 2525 Bay Area a Gigaman circuit is used to connect Barrios and other contractors back to the ISOLAN.

JAXA	JAXA	The JAXA network interfaces with JSC through NASA provided Cisco wireless bridges between the Cyberonics Bldg located in 16511 Space Center Blvd. and 2525 Bay Area Blvd. At 2525 Bay Area a Gigaman circuit is used to connect JAXA and other contractors back to the ISOLAN.
Oceaneering	Oceaneering	The Oceaneering network interfaces with JSC through NASA provided Cisco wireless bridges between their building located on Space Center Blvd. and 2525 Bay Area Blvd. At 2525 Bay Area a Gigaman circuit is used to connect Oceaneering and other contractors back to the ISOLAN.
Booz Allen Hamilton	Booz Allen Hamilton	The Booz Allen Hamilton network interfaces with JSC through NASA provided Gigaman circuit at 2525 Bay Area. This circuit is shared with other contractors in the area to connect back to the ISOLAN.
Honeywell	Honeywell	The Honeywell network interfaces with JSC through NASA provided Gigaman circuit at 2525 Bay Area. This circuit is shared with other contractors in the area to connect back to the ISOLAN.
Futron	Futron	The Futron network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
Titan	Titan	The Titan network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
GEOCONTROL	GEOCONTROL	The Geocontrol network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
Raytheon	Raytheon	The Raytheon network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
JIMMS	JIMMS	The JIMMS network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
INDYNE	INDYNE	The Indyne network interfaces with JSC through NASA provided Cisco wireless

		bridges between their building and JSC ISOLAN.
Jacobs Engineering	Jacobs Engineering	Jacobs Sverdrup interfaces with JSC via a NASA-provided high speed wireless network between their building and JSC ISOLAN.
Draper Labs	Draper Labs	The Draper network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
Bastion	Bastion	The Bastion network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
Wyle	Wyle	The Wyle network interfaces with JSC through NASA provided Cisco wireless bridges between their building at Parsec II and JSC ISOLAN.
Blackhawk	Blackhawk	The Blackhawk network interfaces with JSC through NASA provided Cisco wireless bridges between their building and JSC ISOLAN.
Regents Park 3	United Space Alliance (USA)	The conference facility at Regents Park III connects to JSC ISOLAN via a NASA provided wireless bridge.
1120 NASA Parkway	Akima, Odyssey (EA contractor)	The Akima and Odyssey contractor networks connect to JSC ISOLAN via a NASA provided wireless bridge.
2200 Space Park Dr	TTI, GBTech, Hamilton Sundstrand	The TTI, GBTech, and Hamiliton Sundstrand contractor networks connect to the JSC ISOLAN via a NASA provided wireless bridge.

Internal

EC LAN Subnet 156 (OASIS Network)	Jacobs Engineering through NASA Org EC contract	Non IRD maintained network located primarily in B7 but extends to B31 and B32 through non IRD maintained fiber. Connection to the JSC institutional network is done through router serving B7. Lab uses JSC assigned IP address space.
SSTF Network	DA Org	Non IRD maintained network located in B5S room 3100. Lab uses JSC assigned IP address space.
TAMS Network	DA Org	Non IRD maintained network located in B5S. Lab uses JSC assigned IP address space.
HST RNS Network	Hubble	Non IRD maintained network located in B5N room 117A. Lab uses JSC assigned IP address space.
MER LAB	DA Org	Non IRD maintained network located in B4S. Lab uses JSC assigned IP address space.
MER Network	DA Org	Non IRD maintained network located in B4S. Lab uses JSC assigned IP address space.
USA FOT Network	United Space Alliance (USA) DA Org	Non IRD maintained network located in B4S. Lab uses JSC assigned IP address space.
PTT LAB	DA Org	Non IRD maintained network located in B4S. Lab uses JSC assigned IP address space.
STEALTH/COSS LAB	MA	Non IRD maintained network located in B4S. Lab uses JSC assigned IP address space.
B9 ISL LAN	DA	Non IRD maintained network located in B9. Lab uses JSC assigned IP address space.
SSMTF LAN	DA	Non IRD maintained network located in B9. Lab uses JSC assigned IP address space.
B9/2115	DA	Non IRD maintained network located in B9. Lab uses JSC assigned IP address space.
BIO LAN	Jacobs Engineering	Non IRD maintained network located in B10. Lab uses JSC assigned IP address space.
EC LAB	EA	Non IRD maintained network located in B13 room 2008. Lab uses JSC assigned IP address space.
CEL LAB	EA	Non IRD maintained network located in B15 room 2E2. Lab uses JSC assigned IP address space.
ER1 Lab	EA	Non IRD maintained network located in B16 room 179. Lab uses JSC assigned IP address space.
ASDEP Network	EA	Non IRD maintained network located in B16. Lab uses JSC assigned IP address space.

SES Network	EA	Non IRD maintained network located in B16. Lab uses JSC assigned IP address space.
EV LAB	EA	Non IRD maintained network located in B16A room 1153A. Lab uses JSC assigned IP address space.
Jupiter Lab	DA	Non IRD maintained network located in B30A room 2069. Lab uses JSC assigned IP address space.
DA9 Lab	DA	Non IRD maintained network located in B30A room 1043. Lab uses JSC assigned IP address space.
CSOC LAB	DA	Non IRD maintained network located in B30A room 3058. Lab uses JSC assigned IP address space.
IPAD LAB	DA	Non IRD maintained network located in B30A room 3000. Lab uses JSC assigned IP address space.
MSL/ODRC EXT	DA	Non IRD maintained network located in B30M room 116. Lab uses JSC assigned IP address space.
SDFC LAN	DA	Non IRD maintained network located in B30. Lab uses JSC assigned IP address space.
MIDDS	DA	Non IRD maintained network located in B30M room 127. Lab uses JSC assigned IP address space.
IPS/SSEE	DA	Non IRD maintained network located in B30S room 5301. Lab uses JSC assigned IP address space.
E-POC	DA	Non IRD maintained network located in B30S room3301D. Lab uses JSC assigned IP address space.
ISL LAB	DA	Non IRD maintained network located in B32 room 218A. Lab uses JSC assigned IP address space.
CDPA LAN	DA	Non IRD maintained network located in B35. Lab uses JSC assigned IP address space.
Lockheed LAN	Lockheed Martin	Non IRD maintained network located in B10. Lab uses JSC assigned IP address space.
IRD LAB	NASA IRD	IRD Lab for new technology development and testing. Lab is located in B46.
IRD SEB	NASA IRD	Source board networks. Area located in B46.
USA Maintained Network	United Space Alliance (USA)	Non IRD maintained network located in B46. Lab uses JSC assigned IP address space.
CMIS/NICE Network	NASA IRD	Constellation Imagery network. Network extends from B46 to B8 through a backend 10G infrastructure.
DDMS Network	NASA IRD	
Credit Card POS B3	AH	Non IRD maintained network located in B3 Cafeteria. Lab uses JSC assigned IP address space.
Credit Card POS	AH	Non IRD maintained network located in B11 Cafeteria. Lab

B11		uses JSC assigned IP address space.
IRD SEB	NASA IRD	Source board network. Area located in B265.
IRD SEB	NASA IRD	Source board network. Area located in B269.
IRD SEB	NASA IRD	Source board network. Area located in B259.
IRD SEB	NASA IRD	Source board network. Area located in B225.
B343 LAB	JA	Non IRD maintained network located in B343. Lab uses JSC assigned IP address space.
IRD SEB	NASA IRD	Source board network. Area located in B416.
SDIL	OA	Non IRD maintained network located in Sonny Carter Training Facility (SCTF). Lab uses JSC assigned IP address space.
SDIL to PDL	OA	Non IRD maintained network located in Sonny Carter Training Facility (SCTF). Lab uses JSC assigned IP address space.
DRR LAB	OA	Non IRD maintained network located in Sonny Carter Training Facility (SCTF). Lab uses JSC assigned IP address space.
DRATS LAN	EA, DA	Non IRD maintained network located behind building X (B220). LAN uses JSC assigned IP address space.

4.7.12 IT Security

The NICS contractor will be responsible for providing IT security for the equipment maintained under the NICS contract. The NICS contractor will also interface with the SOC, local ITSM and the local IT security contractor, currently performed by the JETS contract.

4.7.13 Cable Plant Services

JSC cable plant includes fiber optic and copper cabling, both inter-building and intra-building. JSC has a tunnel system that connects much of the main campus buildings for utilities such as power and water. Inter-building fiber optic cabling and copper cabling is installed in trays throughout the JSC tunnel system. Some cabling is direct buried or buried in conduit with access manholes and hand-boxes spaced out along the path of the cabling. JSC has extensive copper outside cable plant that is buried and contains many pedestals throughout the campus. JSC confined space training (renewable every 24 months) is required for working in the JSC tunnel system and manholes. JSC confined space training is offered monthly at the JSC Safety Learning Center.

4.7.13.1 Optical Fiber

JSC primarily uses single mode fiber between buildings on the JSC campus. In general, there are 36 strands of single-mode fiber from each major building to the core locations. Also, there are 144 strands of single-mode fiber between core locations Buildings 46, 17 and 32A. There are also 288 strands of single-mode fiber from the 200, 300, and 400 area buildings to core locations in Building 46 and 32. Many buildings have been outfitted single-mode fiber within the building, and all new installations of fiber optic cabling at JSC will be single-mode fiber.

JSC uses multi-mode fiber within many of the buildings on the campus, as well as between some buildings in the 300 and 400 building area. Since multi-mode fiber is best suited for use in short lengths, JSC is replacing the multi-mode fiber whenever possible with single mode fiber.

4.7.13.2 Twisted Pair Copper Cabling

JSC uses Category 5E unshielded twisted pair copper cable for all data and telephone network end user cabling.

4.7.14 Emergency Warning Systems (RESERVED)

4.7.15 Public Address Systems (RESERVED)

4.7.16 Radio Services (RESERVED)

4.7.17 Telephone Services

The following information describes the telephone systems at JSC and its associated component facilities, as well as the separate telephone system that provides service for WSTF.

4.7.17.1 System Overview

The JSC telephone system is called the Center Telecommunications System (CTS) and it consists of a multi-node Siemens EWSD™. It is connected to public telecommunications facilities via approximately 25 PRI trunks, with the host switching unit located in JSC Building 17 and remote switching units (RSU) at JSC Building 30A, Ellington Field and Sonny Carter Training Facility. The host switching units is backed up by facility UPS and diesel generator. Building 30A RSU supports the JSC Mission Control Center and is also protected via UPS and generator. Services provided include voicemail, caller ID, call-forwarding, conference calling, speed-dial, 5-digit dialing for all JSC locations supported by the Siemens system, and long distance, which is provided by the Networx contract.

The Direct Inward Dial numbers for JSC, Ellington, and Sonny Carter Training Facility are:

a) 281-483-XXXX, Five digit dialing: 3XXXX
b) 281-244-XXXX, Five digit dialing: 4XXXX
c) 281-792-XXXX, Five digit dialing: 2XXXX

WSTF has three Nortel Option 61C PBX Switches. The Primary and Secondary switches support the WSTF main campus, and the third switch resides at WSSH. The WSTF telephone system uses the WSTF fiber and copper cable plant, and serves approximately 40 buildings with around 1000 telephones. The primary switch is located in the WSTF Data Center facility, which has a UPS and generator backup.

Both the JSC and WSTF telephone systems support custom circuits for paging, alarm, crash network and other circuits, including point to point data circuits. The ODIN contract provides five types of telephone service seats:

a) PH1 – Analog line Services
b) PH3 - Standard Desktop Phone Services
c) PH4 - Conference Room Phone Services
d) PH5 - Point to Point Communication Circuit Services (connecting customer owned devices)
e) PH6 - Point to Point Communication Circuit Services (connecting the Center telephone switch to customer's device)

4.7.17.2 Handsets

JSC uses Siemens Optiset ISDN telephones for most of the campus. The Siemen's Optiset ISDN phone uses a premises powering unit that integrates NT1 caging, 48 volt DC power, and battery backup in a single unit for powering the Optiset ISDN telephones. The PR300-U is available in four models that house and power 12 to 48 NT1's and provide power for 24 to 96 phones in a multipoint mode. In addition, the 24 and 72 line versions of the PR300 are field upgradeable by adding a 300R-U NT1 cage. The PoweRack 300-U can be either wall or rack mounted. During extended periods of utility outage the batteries are protected from over-discharge by the built-in low voltage detector and disconnect circuit. Some telephones Northern Telecom analog only phones, mostly in areas where there are 6 or less telephones deployed. Conference room telephones are typically Polycom brand speaker phones that are connected to the Siemens switch via analog lines. There are approximately 18,000 telephones of all types across the JSC campus and associated facilities (except WSTF, whish has a separate phone system).

The standard practice at JSC has been that if you are a civil servant or on-site contractor, you would keep your current phone number if relocated to or from another JSC building including Ellington Field and Sonny Carter Training Facility.

WSTF uses Nortel handsets for their telephone system, and there are approximately 1000 telephones at WSTF.

4.7.17.3 Voicemail Services

The Siemens telephone system provides voicemail for all users that sign up for the voicemail option on the ODIN phone seat. Voicemail options are Regular and Enhanced. Regular voicemail provides 10 messages that can be 90 seconds in length. Enhanced voicemail provides 20 messages that can be 90 seconds in length.

The WSTF voicemail system is a Nortel Standard Voicemail system.

4.7.17.4 E-911 Services

The JSC telephone numbers are all tracked by ODIN via a database that provides information to the JSC Emergency Operations Center (EOC) in the event of an emergency call. Information provided includes telephone number, assigned user, and building and room identifiers.

4.7.17.5 Trunks

There are approximately 23 PRI trunks connecting the JSC Siemens EWSD host and remote switching units to the public telephone infrastructure (local dial-tone).

There are approximately 7 PRI trunks connecting the Nortel systems at WSTF to the public telephone infrastructure.

4.7.18 Voice over Internet Protocol (VoIP)

JSC has a small deployment of Cisco Voice over Internet Protocol technology. The equipment that comprises the JSC VoIP system includes:

a) 2 Call Processing Servers (Cisco Call Manager)
b) 2 Cisco 3800 routers acting as IP telephony gateways, each currently configured with 2 PRI interfaces that are connected to the legacy JSC telephone system
c) 1 Voicemail Server (Cisco Unity)
d) 1 Cisco Emergency Responder (CER)
e) Approximately 300 Cisco 79xx series IP Phones
f) 8 Uninterruptible Power Supplies (UPS) (Located in Buildings 1, 17, 27, 45, 46, 265, as well as offsite facilities 2200 Space Park Drive and 1100 NASA Parkway)

JSC uses Quality of Service (QoS) to prioritize voice traffic on the network, specifically, Cisco's AutoQoS technology.

The current plan is that any areas of the JSC campus that are refurbished, renovation, or new construction would be outfitted with VoIP telephones, so the VoIP system is designed to grow up to 1000 phones with the current equipment. Full conversion to VoIP is currently planned to occur in 2014, when the current legacy JSC telephone will have been in service for 14 years.

WSTF currently uses the JSC Call Manager under a prototype configuration. It supports approx 10 VOIP phones. Similar to the JSC, WSTF will continue to move toward VOIP infrastructure as the most likely replacement for the existing legacy telephone system, with the expectation that the replacement will be scheduled in conjunction with the JSC legacy telephone system replacement. WSTF expects to support all current existing voice services under the VOIP infrastructure and be capable of working as a standalone environment in the event JSC systems are not available.

4.7.19 Cable Television Services (RESERVED)

4.7.20 Continuation of Center Zoned Architecture Project (CZAP)

The JSC NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.7.21 Ongoing Center-Specific Projects

The following JSC and WSTF projects will either be in progress at the start of NICS or are planned to occur during the NICS contract:

a) JSC Building Refurbishment – JSC has an ongoing project that is expected to last for the next twenty years to refurbish most of the main campus buildings. This project, being run by the Center Operations Directorate (COD), will involve gutting each building and constructing it anew, meeting current building codes and delivering on government goals for creating and using green facilities. As each building is redone, the occupants must move to a different facility temporarily, and then be moved back to the facility after construction is complete. The NICS contractor will have to support the IT needs of moving employees, removal of IT infrastructure from construction areas, re-installation of infrastructure, and supporting moving employees into the completed facilities. To aid in this work, a new office building that will hold about 500 displaced employees is being constructed onsite, to be completed in calendar year 2010. The IT infrastructure to support this new building is likely going to be in progress during the phase-in of NICS, which will have to pick up the work from the incumbent contractor. In the recent past as the refurbishment began, in lieu of having an onsite facility to move displaced employees, offsite space has been leased to provide a temporary relocation facility for

employees. The offsite lease space was treated as if it were on-site from an IT infrastructure perspective.

b) JSC Telephone System Replacement – It is currently planned that JSC will replace its Siemens telephone system (and WSTF's Nortel system) around FY2014. The expectation is that by that time, the JSC network will be able to fully support VoIP with distribution layer redundancy, power over Ethernet, Quality of Service, etc. Also, the JSC phone system will have reached its end of life, which is projected at about 15 years.

4.7.22 Work Load Indicators

4.7.22.1 JSC Workload Indicators

PWS Section	Indicator	2007 Approximate Quantities/month	2008 Approximate Quantities / Month
3.1.1	IPAM data updates		
3.1.2	New or updated remote access accounts	20	30
3.1.4	Number of guest accounts		
3.6	Network trouble tickets	289	541
3.6	Network MAC	599	718
3.6	Network service requests		
3.12	IT security incident response support		
3.12	Firewall rule changes		
3.12	Security documentation packages		
4.x.5	Telephone trouble tickets	241	270
4.x.5	Telephone MAC	311	365
4.x.5	Telephone service requests		
5.0	Network projects greater than $500K	Network Hardware Replacements each year	Network Hardware Replacements each year

4.7.22.2 WSTF Workload Indicators

PWS Section	Indicator	2007 Approximate Quantities/month	2008 Approximate Quantities / Month
3.1.1	IPAM data updates		
3.1.2	New or updated remote access accounts		
3.1.4	Number of guest accounts		
3.6	Network trouble tickets	10	10
3.6	Network MAC	5	5
3.6	Network service requests		
3.12	IT security incident response support		
3.12	Firewall rule changes		
3.12	Security documentation packages		
4.x.5	Telephone trouble tickets		
4.x.5	Telephone MAC	20	20
4.x.5	Telephone service requests		
5.0	Network projects greater than $500K		

4.7.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.8 KENNEDY SPACE CENTER (KSC)

KSC encompasses over 140,000 acres of which 15,000 acres are populated by approximately 15,000 civil servants and contractor employees. NICS network services will be delivered to over 240 facilities across the entire geographical area. Additionally, services are provided to multiple remote NASA occupied facilities at Cape Canaveral Air Force Station/Patrick Air Force Base (CCAFS/PAFB), various facilities near KSC and other locations as specified in the contract. This includes supported devices at Vandenberg Air Force Base (VAFB) in Lompoc, CA, and remote resident offices across the United States, currently in Littleton, Co, Sterling, VA, and Chandler, AZ.

This contract will deliver products and services to multiple National Aeronautics and Space Administration (NASA) programs, the Department of Defense (DoD), contractors, academia, other Government agencies located on center, world-wide news media organizations, and varied space related industry entities. The contractor plans, designs, implements, maintains, operates, sustains, and provides life cycle management for these products and services to ensure the highest availability, integrity, and security.

The Information Management and Communications Support (IMCS) contract is the Center's incumbent primary provider of information technology and communication services for the Kennedy Space Center (KSC). NICS is expected to coordinate with IMCS for communication support in the areas not supported by the NICS contract at this location.

During the contract performance period, the composition of NASA's mission and budget will change significantly as the Shuttle program winds down and the follow-on activities commence. It is expected that the contractor will have the flexibility to remain responsive to contract requirements resulting from such changes.

4.8.1 Property/Inventory

The contractor currently is responsible for providing property management functions which support the internal KSC Networking & Communications organizations (NASA IT & IMCS) as they provide services detailed in the PWS.

This includes assuming management of the currently identified inventory of all hardware and software as listed in the NICS Government-Furnished Property (GFP) Appendices, and provides property management, utilizing the NASA Property Management System (N-PROP) to track and manage government tagged property. The incumbent contractor currently utilizes the KSC Maximo system as the primary asset management tool for items not required to be tracked via NPROP.

The contractor also identifies and provides critical spares, bench stock, consumables and associated equipment, and materials required to meet the requirements of this contract, and purchases supplies and services to accomplish assigned work on the current KSC Networking and communications contract (IMCS). Throughout the course of the year, the contractor also

performs periodic surveys to validate the status of the current property, identifies any equipment "found on station" and provides inputs regarding any equipment designated lost

In an attempt to perform the contractual duties in the most efficient manner possible, the contractor also monitors the identified government excess channels to any equipment that is designated on a local "watch list" for potential use in the implementation, operations & maintenance of the designated systems as defined by the existing contract

Finally, the current contractor identifies excess and obsolete out-of-service assets, and initiates disposal per Agency and KSC guidelines, policies, and directives. This includes ensuring that all items removed from service have all data removed prior to excess in accordance with applicable KSC and Agency policies and procedures.

The contractor also currently operates an on-site Material Service Centers in support of internal work processes for the organizations. This includes the storage of all hardware, software, and other associated equipment in accordance with manufacturer's storage specifications and recommendations that meet Agency and KSC guidelines, policies, and directives. Upon receipt of returned/repaired equipment, the contractor ensures that the equipment is repaired and returned to stock to ensure no impact to operations.

4.8.2 Shipping/Receiving/Inspection Services

The current KSC contractor is responsible for utilizing government-provided storage facilities for storage of all hardware, software, and other associated equipment to meet the requirements of this contract. In performance of these services, the contractor prepares items for shipping, with adequate documentation, as required by the Government-furnished services (GFS) shipping service provider. This includes the management of any existing property tags permanently affixed to all existing assets.

In receiving supplies or equipment in support of the current contract, the current contractor provides receiving and inspection functions including accountability, storage and warehousing support. As required, the contractor also works with the center property control personnel to manage Government provided NASA Equipment Control Number (ECN) tags and decals for acquired or procured equipment that meet the designated criteria for government tagged equipment.

4.8.3 Vehicle Management

The current contractor is responsible for performing vehicle management functions in accordance with NPR 6200.1, *NASA Transportation and General Traffic Management*; NPD 6000.1, *Transportation Management*; and KNPR 6000.1, *Transportation Support System Manual*, and Executive Order 13423, *Strengthening Federal, Environmental, Energy, and Transportation Management*. In performance of the current KSC networking support services, the contractor furnishes and maintains all general purpose vehicles in support of current contract requirements. GSA schedules are utilized to satisfy the requirements for motor vehicles at the discretion of the contractor. The contractor also operate NASA-owned or leased vehicles and utilizes KSC on-site fueling stations for fueling general purpose vehicles and Government-

furnished vehicles. The contractor organization is responsible for ensure that all drivers have proper state licenses, with the applicable endorsements, for requisite equipment being operated, and inputs any required data into the Federal Automotive Statistical Tool (FAST) for any contractor-acquired or leased and NASA-owned vehicles annually, as scheduled by the KSC NASA vehicle Fleet Manager.

4.8.4 Physical Security

The current KSC contractor operates a security program in accordance with KSC, Agency, DoD, and Department of Homeland Security directives. The contractor complies with requirements regarding sensitive but unclassified (SBU)/Controlled Unclassified Information (CUI) in NPR 1600.1. The contractor develops, implements, and updates an Export Control Plan consistent with applicable KSC, Agency, Department of State, and Department of Commerce regulations and procedures, including identifications a representative to be named to the Center Export Control Working Group (ECWG). The current KSC contractor provide support and information to internal and external auditing and investigations performed by agencies such as General Accounting Office (GAO), Office of the Inspector General (OIG), Defense Contracting Audit Agency (DCAA), Defense Contract Management Agency (DCMA), Federal Bureau of Investigation (FBI), Office of Management and Budget (OMB), independent boards, and other requests as required.

The current contractor also performs tasks related to the physical access management elements of the areas supported by the contract, including the key management for the assigned lock cores/keys related to the assigned physical areas, in concert with the designated facility managers.

4.8.5 Emergency Management

The current KSC communications contractor has developed, implemented and continues to update a Center level Emergency Preparedness Plan in compliance with Joint Handbook (JHB) 2000, *Consolidated Comprehensive Emergency Management Plan,* and includes the contractor's assigned systems, hardware, software, infrastructure, equipment, data storage, and operations.

The primary function of the emergency management plan is to ensure that the Emergency Preparedness Plan includes scenarios to respond to significant loss of capability due to accident or incident, equipment or infrastructure failures, attacks against computer systems and networks, loss of capability due to natural disaster, and other Center-level emergency situations and include plans to conduct timely recovery during these contingencies. The plan includes the contractor's approach to implementing specific protective and preventative measures for the contractor's assigned facilities, systems, equipment, and operations, and mission specific requirements are addressed where applicable. The current contractor supports the emergency preparation/recovery activities, including responding and implementing real-time identified requirements at the direction of the CO, COTR, or designee under Center, Program or Agency declared emergency

conditions. These preparation activities include planning for and participating in drills, as well as implementing the respective Emergency Preparedness Plan for declared emergencies.

The contractor participates in on-going Emergency Management Plan maintenance and modifications for the relevant sections of the D9001, *Comm. Systems Hurricane Preparedness Procedures*, for all services provided in performance of this existing contract.

The current contractor has also designated an on-site contractor Emergency Coordinator responsible for supporting emergency preparedness planning and implementation, who interfaces with the KSC Emergency Preparedness Officer, as well as leads immediate action to eliminate hazards to personnel, equipment or environment; prevent loss of or damage to Government property; and restore essential services following a declared emergency condition.

4.8.5.1 Center Specific COOP Support

The current contractor has developed sections of the KSC Continuity of Operations Plan (COOP) compliant with NASA NPD 1040.4A and NPR 1040.1, and integrated with the other elements of the KSC Information Technology Communications Service Delivery. The primary plan may utilize elements from KSC document number D9001, Comm. Systems Hurricane Preparedness Procedures. At least annually, the contractor will test the COOP as defined in NPR 1040.1 and provide documented results to the Government per COOP Annual Test Report format.

4.8.5.2 Service Continuity of Operations Support

The current contractor provides the necessary staffing to support any require service continuity of operation activities. This would include the most common scenarios experienced at Kennedy Space Center, including the activation of the KSC Hurricane Condition (HURCON), and the execution of the related Communications Systems Hurricane Preparedness Procedures.

4.8.6 Safety

The current networking contractor (as part of the KSC Information Management and Communications Services contract) is responsible for providing safe programs, technologies, operations, and systems to ensure the protection of the public, Astronauts and pilots, Government and contractor workforce, and high-value equipment and property at the Kennedy Space Center and its associated component facilities in the performance of its contractual duties.

Correspondingly, the contractor is taking all reasonable safety and health measures in performing the existing contract tasks to assure the protection of employees and property as described in NFS 1852.223-70, *Safety and Health*. This includes maintaining technical cognizance of any proposed and implemented changes to all applicable Federal, state, and local laws, regulations, policies, and directives, as well as industry standards, and identify impacts to contractor safety and health requirements, processes, and practices. The contractor is also maintaining safe and healthful operating locations, being proactive in the protection of personnel and property, providing the Government, or authorized contractor representative, immediate access to the sites or areas where work under this contract is being performed in order to conduct surveillance

activities and determine the adequacy of the safety, health, and mission assurance programs, as well as providing all necessary records, including internal audit and assessment results and surveillance activities, to the Government for review as required. The current contractor has also established and maintains a comprehensive safety and health program that meets requirements as defined in NPR 8715.3B, *NASA General Safety Program Requirements*; KNPR 8715.3, *KSC Safety Practices Procedural Requirements*; and Air Force Range Command Range Safety Manual (AFSPCMAN) 91-710 V6, *Ground and Launch Personnel, Equipment, Systems, and Materials Operations Safety Requirements.* To minimize any potential conflicts of interest, the current contract structure is such that it ensures the safety organization maintains independence from the work performing organizations, and supports independent Government audit and surveillance activities of contractor safety and health programs.

From a Safety Compliance perspective, the current KSC contractor is ultimately responsible for providing a safe and healthful work environment and the performance of all activities in a safe manner, they have established a safety and health program throughout all organizations of the contract including major subcontractors to comply with the Occupational Safety and Health Administration (OSHA) Voluntary Protection Program (VPP) Star Program requirements and submitted a VPP Application. They have also developed, implemented and maintain a Safety and Health Plan as required by NFS 1852.223-73, *Safety and Health Plan*, including sections that address confined space entry compliance. They are ensuring all contractor equipment, including equipment owned, assigned, leased, rented, or obtained from off-site locations is properly assembled, maintained, and safe for use, that each employee receives all required Federal or NASA initial and recurring safety and health training and maintain evidence that this required training has been completed and is current. This includes an annual preparation and submittal of a Safety Program Evaluation

From an Occupation Safety perspective, the current contractor is responsible for ensuring a safe working environment by identifying, documenting, mitigating, and preventing workplace hazards, and ensuring the safe condition of assigned systems and equipment. To ensure the current contractor's safety and health requirements are being met, policies, methodology, and procedures have been developed for the protection of personnel.

This includes the completion of safety and health inspections per OSHA VPP, NASA, and KSC safety and health requirements of all contractor-occupied work areas. At least one inspection per year is being performed using qualified contractor safety professionals, which document all inspection findings, track these finding to closure, and communicate to appropriate Government entities regarding the results and current status.

The current KSC networking and communication contractor documents all mishaps, including injuries, property damages, close calls, and corrective actions into the NASA mishap-reporting database. Mishap reporting methods have been implemented and timelines and ensure data accuracy per KNPR 8715.3, *KSC Safety Practices Procedural Requirements*, and submit Mishap Reports (DRD-SH-04). Type C and D mishaps and close calls are investigated and corrective action implemented within 30 calendar days.

These mishap investigations are conducted per NPR 8621.1, *NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping*. In the event of a

Government mishap investigation, the contractor supports the investigation and makes available all pertinent documentation and personnel, as requested. The current contractor also regularly submits a Safety Statistics Report, as well as any safety variance requests for any waivers or deviations from a safety or health requirement to the Government for approval. All variance requests are processed through the appropriate variance review and approval system in accordance with KNPR 8715.3, *KSC Safety Practices Procedural Requirements,* and AFSPCMAN 91-710 V6, *Ground and Launch Personnel, Equipment, Systems, and Materials Operations Safety Requirements.* Risk assessments for all variances requested are performed to assure the safety of personnel and equipment is not compromised. The contractor also evaluates alternate work procedures as a result of a variance prior to implementation.

Furthermore, the contractor ensure current Material Safety Data Sheets (MSDS) are readily available and reviewed by employees for materials used in the workplace, and that employees are protected from serious workplace injury and/or illness resulting from contact with chemical, radiological, physical, electrical, mechanical, or other workplace hazards per KNPR 8715.5, *KSC Personal Protective Equipment (PPE) Program.* The current contractor develops and maintains written procedures for operations and equipment involving the use, exposure to, generation of, or control of occupational health hazards. This includes identifying the hazards in written procedures and including instructions on use of required engineering controls and work practices, including required Personnel Protective Equipment (PPE). This also covers providing employees with the appropriate training and orientation to identify occupational health hazards in all work places and the protective measures required for safety, and notifying employees of any changes or modifications to policies, procedures, or systems used to control exposure to health hazards. Finally, the current contractor monitors and maintains accurate records of employees work hours, including forecasting work schedules, to ensure maximum work-time compliance, per the applicable guidance.

From an Operations Safety Perspective, the current contractor is responsible for providing employees with a workplace in which hazards are identified, evaluated, and eliminated or controlled. Activities associated with this contract will comply with KNPR 8715.3, *KSC Safety Practices Procedural Requirements,* AFSPCMAN 91-710 V6, *Ground and Launch Personnel, Equipment, Systems, and Materials Operations Safety Requirements,* and Federal, NASA, state, and local regulatory safety and health requirements. The contractor perform safety assessments of all hazardous operations, high risk operations, and for first use of new and modified systems and equipment, and identifies all hazards and appropriate mitigation, along with submit any new and revised assessments to NASA Institutional Safety for concurrence. The current contractor develops and maintain technical operating procedures for operations, planned or unplanned, which are hazardous or constitute a potential operational constraint.

The current contractor also ensures compliance with the KSC Lockout/Tagout Program for control of hazardous energy as described in KNPR 8715.4, *KSC Lockout/Tagout Program Procedural Requirements,* and manages entry into and work in confined spaces, in accordance with the requirements of KNPR 1820.4, *KSC Respiratory Protection Program*, KNPR 1840.19, *KSC Industrial Hygiene Programs.*

Finally, the current contractor complies with the NASA Managed Safety Program for Pressure Vessels and Pressure Systems in accordance with NPD 8710.5, *NASA Safety Policy for Pressure Vessels and Pressurized Systems*, and ensures compliance with NASA-STD-8719.9, *Standard for Lifting Devices and Equipment*.

In the area of Environmental Management, the contractor is responsible for ensuring that operations of assigned systems and equipment are in compliance with applicable Federal, state, and local environmental laws, regulations, Executive Orders, and NASA requirements per KNPR 8500.1, *KSC Environmental Requirements*. The NASA Environmental Program Branch is the single point of contact with all regulatory agencies concerning NASA issues such as: regulatory interpretation, compliance reporting, inspections, and spills or releases.

In performance of these services, the contractor supports the NASA environmental program requirements applicable to the contractor, including response to environmental data calls; support to internal and external inspections and audits; providing support to required permit applications and environmental permits; and providing technical support to contractor operations to meet environmental permit and regulatory requirements. This includes ensuring compliance with all environmental regulations, permits and licenses required by the Federal, State, or local governments or a subdivision thereof, or of any duly constituted public authority in performance of work, appointing in writing a primary and alternate Environmental representative for the contract. The contractor ensures that all employees are aware of the Environmental representative and that individual's responsibilities, and the individuals in this position have adequate awareness training to accomplish the assigned duties including hazardous and controlled waste management requirements. Also, the current contractor identifies, interprets, and applies new and existing environmental requirements with respect to contractor operations, prepares environmental reports for permitted activities and regulatory requirements if applicable, responds to Government data calls for chemical usage and storage records for each calendar year, performs waste minimization and pollution prevention opportunity assessments such as reducing Toxic Releases Inventory (TRI) chemical releases and hazardous waste, complies with NASA's affirmative procurement program for contractor procurements in accordance with KNPR 8500.1, *KSC Environmental Requirements* in and Executive Order EO13423, *Strengthening Federal Environmental, Energy, and Transportation Management, and* supports NASA's Environmental Management Systems, and promote environmental awareness within the contractor workforce.

4.8.7 Facilities

Personnel in the related contracts currently occupy on-site space at KSC primarily in 5 buildings, not including any "lights-out" communications rooms/spaces. The following is a quantity listing by type of space.

Type of Space	SQUARE FOOTAGE
Office Space	5900

Technical Space	4100
Storage	3000
Lab	250
Conference Room	400
Miscellaneous	0

Any Required Facility services are currently provided by the Institutional Support Contract (ISC).

4.8.8 Network Services

4.8.8.1 IPAM

The current contractor supported Domain Name Services infrastructure is that of the Agency IPAM system as of April 2009. There are approximately 8 DNS Server nodes supported at KSC, with an additional IPAM DNS server node physically located at Vandenberg Air Force Base in Lompoc, CA. These DNS servers function in 3 primary "clusters", 2 of them providing services to the Internal KSC network, and one of them providing "Open/Public/Guest" services to the KSC Open Network. These nodes are located in the CD&SC (2), VABR (2), CIF, O&C, SSPF, CCFAS Hangar AE, and Building 836 of VAFB.

The current contractor supported DHCP service is delivered via the Agency IPAM system as of April 2009. There are approximately 11 nodes providing DHCP services. Of these 10 nodes, 9 of them "overlap" the DNS node/appliances described above.

These nodes are located in the CD&SC (3), VABR (3), CIF, O&C, SSPF, and CCFAS Hangar AE, and deliver services to multiple environments in the KSC Internal & Open Networks.

4.8.8.2 Remote Access Services

The KSC Secure Remote Access Services (SRAS) subsystem is a collection of remote access services that permit access to the KSC/NASA IT infrastructure from locations external to the Center. These remote access services include basic dial-in modem access service via analog Plain Old Telephone Service (POTS)/ISDN digital lines and redundant dial-in servers (Cisco 37xx class routers with single PRI interfaces), a limited services functionality Secure Sockets Layer (SSL) based Virtual Private Networking (VPN) solution using the Agency standard web browsers as access clients (using redundant Juniper Networks Access 6000 series SSL VPN gateways), and an Internet Protocol Security (IPSEC) client based VPN gateway services using a set of redundant Cisco 3000 series VPN concentrators. This IPSEC client based service provides both full remote host connectivity, as well as a subset of that connectivity to certain remote user groups, based on group access profiles, and ultimately will perform full remote client

configuration auditing via network admission control agents. This full VPN client is supported in Windows, MacOS X, and Linux/Unix environments.

A redundant Remote Authentication Dial-In User Service (RADIUS) system, based on the Juniper/Funk Global Enterprise Edition RADIUS software application running on Intel based server platforms, provides basic DHCP, account logging, and pass-through authentication functions for these SRAS components. Secondary support servers providing Microsoft (MS) Windows Internet Naming Services (WINS) and Domain Name Services are also currently functional within this subsystem.

A two-factor authentication system based on the COTS RSA Security SecurID hardware tokens and redundant ACE servers running on Solaris based servers provides two factor authentication for the SRAS servers. Although this system primarily provides authentication for the SRAS components, it also provides strong authentication for selected systems across the Center, such as the KSC "TechDoc" document management system, and the Agency Security Update Service (ASUS). These two-factor strong authentication services are also utilized with the on-board ACE Server TACACS+ server daemon built into the redundant ACE Servers to provide centralized strong network authentication to the individual components of the Network Security Perimeter. These services will ultimately be provided by another one of the I^3P contracts to this subsystem.

A series of network monitoring & reporting application provides a more user friendly reporting function over the built in reporting functions of the servers. A SRAS support web server that provides some user self service token management functions and an SRAS client download repository is also operational.

Two redundant instances of the RADIUS are functional in different facilities with one in the CD&SC and one in the CIF KNET Control Center on separate "Center services" network segments and adjacent to other key network services nodes.

These RADIUS servers interface with the Center provided Services. The Center services network segment in the CD&SC includes a small Blue Coat Systems proxy server providing external http/https connectivity for a limited number of on-site networks/hosts that would not otherwise be routed off-site as a NASA managed network.

Within the NSP management and monitoring subsystem, there are a number of sub-functions that are performed by multiple components within this logical grouping.

4.8.8.3 Network Time Protocol (NTP)

The current contractor provides a center-wide Network Time Protocol (NTP) service as an extension of the KSC/Range Timing system, which employs redundant Cesium Clock references for a highly accurate time reference signal. This KSC timing signal is translated to a Network Time Protocol signal via 4 redundant Truetime and Symmetricom Appliances (2 in each major communication hub facility) that can provide Stratum 1 timing references to the network attached devices. This is done as an exception to the standardized NASA Integrated Services

Network (NISN) delivered timing system, which only employs the less accurate Global Positioning System (GPS) based time references at the majority of its locations.

4.8.8.4 Guest Network

The Kennedy Space Center Guest Network is delivered via the Open/Public Network segments across the Kennedy Space Center, Cape Canaveral Air Force Station, and Vandenberg Air Force Base in Lompoc, CA as an extended campus of KSC. This network, comprised of both wired and wireless services, is available in a number of the facilities at this time, although not all facilities. It is delivered through a mix of Virtual Local Area Networks (VLANs), Policy based Routing, as well as some dedicated physical networks. Access is currently limited largely by physical access, and no special guest account is currently required, although this may change to an "authentication portal" type of solution in the near future, based on Agency requirements. A Guest network interface point to the "near site" Astrotech Payload Processing facility in nearby Titusville, FL has been established as well to support the NASA processing of payloads while at this facility, although the LANs at that location are supported by the Astrotech personnel. This network sits behind an Open/Public Firewall managed by the local network personnel, and is connected to the Center's border router logically outside the Internal Center Firewalls.

4.8.9 Data Services

4.8.9.1 High Level LAN Description

KNET provides approximately 20,000 network connections across the multiple campuses that it supports. KNET currently supports exclusively IP based protocols and is controlled using approximately 30 routers, 600 switches/hubs and 550 access points to provide networking to over 240 buildings and trailers throughout KSC , NASA occupied facilities on CCAFS/PAFB, VAFB and the remote resident offices . KNET also supports various offsite facilities in the immediate vicinity of Kennedy Space Center. For the NASA facilities located on Vandenberg AFB, the following are currently required/supported:

a) Provide and remotely manage the point of presence in Building 836. Incidental touch labor is provided through an ACA with the Launch Services Program (LSP) managed contractor.
b) Provide and remote management of the wireless equipment
c) Assignment a block of IP addresses for use by NASA and NASA contractors
d) Providing (as required) equipment and installation drawings for incidental system changes. Touch labor is being provided through an ACA with the LSP managed contractor.
e) Management of the NISN network extension between KSC and VAFB for administrative networking on both the OPEN and INTERNAL networks including provisioning routers on both ends, and troubleshooting with NISN on the Wide Area Network link.

f) Performance of on-site installation of major upgrades. Subsequent incidental changes may be accomplished via an ACA with the LSP managed contractor.

For the NASA Launch Services Program Remote Resident office facilities located at Littleton CO, Sterling, VA, and Chandler, AZ, the following is currently supported:

a) Provisioning and remote management of the firewall point of presence at each of the remote resident offices. Incidental touch labor is provided through an ACA with the Launch Services Program (LSP) managed contractor, Expendable Launch Vehicle Integrated Support (ELVIS).
b) Assignment of a block of IP addresses for use by NASA and NASA contractors at these locations
c) Provides (as required) equipment and installation drawings for incidental system changes. Touch labor is being provided through an ACA with the LSP managed contractor.
d) Management of the encrypted network tunnel extension between KSC and these locations for administrative networking on both ends, including provisioning the firewall devices on both ends, and troubleshooting with the wide area network service providers as required.

The current KSC network consists of 100/1000 Mbps Ethernet and associated cable for data transmission to desktop, laptops, servers, VoIP phones, IP cameras, and other end user devices. KNET is built upon and utilizes cabling and communications service capabilities provided by the IMCS contract. KNET sustaining engineering efforts for the wired network include upgrading bandwidth limiting 10Base2/Category 3 cabling to Category 6A premise wiring, and 10 Mbps switches/hubs to 100/1000 Mbps switched Ethernet. Several remote locations at KSC and CCAFS/PAFB where fiber optic cable is not available are served by Digital Subscriber Line (DSL) equipment at lower speeds. KNET also provides wireless LAN service. Wireless LAN Service is provided in most facilities across KSC.

a) KNET interconnects geographically dispersed facilities with a redundant Kennedy Metropolitan Area Network (KMAN) 1 Gigabit Ethernet switched backbone. KNET connects to external providers such as NISN through KMAN and the Network Security Perimeter (NSP).

b) KNET uses policy based routing and virtual LAN's to provide two segmented/logically isolated networks referred to as internal (private), public/open (two islands) across KSC and NASA occupied facilities on CCAFS/PAFB. KNET also has interfaces with multiple Customer Owned and Maintained Networks at all locations.

KNET operates and maintains a number of network services. These include:

a) Authorization, Authentication, and Accounting Service – Cisco Secure Control Server (RADIUS and TACACS+) and Juniper Steel-Belted Radius Server. These are used for the management of the network infrastructure, as well as pass-through authentication of wireless clients on the internal wireless network.

KNET's Network Control Center (NCC) operates from a primary location at the Central Instrumentation Facility (CIF) and a limited functional backup NCC located at the Operations &Checkout building. Network management currently uses software and protocols including, but not limited to:

a) Network Management Application – Cisco CiscoWorks, Cisco Wireless Control Server, Solarwinds Orion, and Ipswitch What's Up Gold

b) Network Operations Database Servers – Microsoft SQL Server

c) Network Web Servers – Microsoft IIS and Apache

d) Network Troubleshooting Tools – Netscout Sniffer, F-Secure SSH Client and File Transfer, and Orion Solarwinds

New or revitalized facilities are typically premises wired with a minimum of one Customer Face Plate per 100 square feet of area. Each CFP delivers 2 Category 6 augmented cabling. Additional CFPs may be installed per user requirements.

The majority of the KNET routers, gateways, switches, and hubs are manufactured by Cisco Systems. However, there many 3COM and Cabletron hubs and switches still operating within the network. The bulk of the wireless devices are manufactured by Cisco Systems. The DSL devices are manufactured by Tut Systems, Pairgain, and Cisco Systems.

4.8.9.2 Wireless Networks

The KSC Wireless networks provide IEEE 802.11b/g networking services in a number of Kennedy Space Center, Cape Canaveral AFS, and Vandenberg AFB facilities.

KNET primarily installs the Cisco 1130, 1140, 1230, 1240, 1250, and 1300 series access points. These access points are connected to a series of Cisco Wireless LAN controllers using the Lightweight Access Point Protocol. The wireless LAN system is managed by the Cisco Wireless Control System application.

Most KSC access points provide wireless connectivity to both the Open (Guest) and Internal (Private) network. The Open Wireless Network is configured with a static 128-bit encryption key to provide some level of security. No authentication is required for the Open wireless service. For the Internal Wireless LAN system, KNET currently provides a pre-WPA and WPA2 solution for connectivity. For the pre-WPA connectivity, KNET uses the Cisco Compatible Extensions (CCX) version 1 to provide security. KNET's configuration for CCX ver. 1 includes LEAP for authentication and TKIP/CKIP for encryption. For the WPA2 solution, KNET uses LEAP for authentication and AES for encryption. LEAP authentication is configured to allow pass-thru authentication to the Center's services provides' (ODIN, USA, Boeing, etc.) active directory service.

KNET also provides wireless service as required for special projects and operational areas.

Future projects include the authentication for the Open wireless users, provide non-proprietary methods (PEAP, TLS) for authentication on the Internal wireless network, and IEEE 802.11a/n service.

4.8.9.3 Network Security

The KSC Network Security Perimeter (NSP) system is comprised of a series of interrelated/interconnected networking, security, and monitoring subsystems that provide a variety of functional services that are both protective and service delivery oriented.

The NSP functions as the primary KSC Wide Area Network (WAN) ingress/egress point to the outside world (including the other NASA Centers, partners, contractors, and the Internet). Via NISN, the NSP delivers primary, first level Center perimeter access control services and provides remote access services, intrusion detection, ingress/egress monitoring, network troubleshooting access, and performance measurement capabilities at the Center's network edge. The primary locations of this system are in the Communications, Distribution & Switching Center (CD&SC) and CIF facilities with secondary monitoring locations in the Headquarters building

The connectivity architecture is a basic three layer external router-firewall-internal router configuration with passive monitoring points located throughout the layers and subsystems to permit the completion of transparent system management, traffic monitoring, and network troubleshooting. Firewall filtering and other forms of traffic intervention are performed in some capacity at every layer of this architecture using "Stateful" network firewalls, router access control lists, and route filtering. Direct interface to a number of "near-site" contractor/partner facilities (e.g. Boeing "Bldg 100," the Astrotech spacecraft processing facility, and the 45th Space Wing network at CCAFS/PAFB) is completed via a dedicated set of partner switches

connected at KSC and remote locations. Additionally, the two major network environments (internal and open/guest) at KSC are defined and delivered to the Center LAN through a variety of logical and physical means.

The routers and switches that interconnect the various system components and functions are a combination of Cisco Catalyst 6500 series, Catalyst 4500 series chassis based switches, Cisco 3700 series based Ethernet routers, and a number of non-modular Cisco Catalyst 35xx and 29xx series switches. These switches and routers are interconnected through a mix of 1 Gbps and 100 Mbps network paths.

The two primary sets of KSC firewalls (for the internal and guest networks) are redundant Checkpoint Firewall NGX-based Intel server platform clusters.

The Remote Resident Office Firewalls at Littleton, Co, Sterling, VA and Chandler, AZ are small office Firewall (Juniper Networks SSG5s) with out-of-band dial backup console port servers connected to them.

The KSC Firewall services are currently managed as a subset of the Network Security Perimeter. The Network Security Perimeter Group also manages a number of (internal) Center Firewalls performing internal system protective functions. These firewalls include the initial KSC Data Center Firewalls (Juniper Networks SSG 550M Cluster), the firewalls for the internal VoIP Call Manager locations at the CD&SC , O&C & Space Life Science Laboratory (Juniper Networks SSG 140s),

The perimeter firewall clusters are supported by a pair of Checkpoint firewall management and logging servers that manage the individual firewall clusters and perform flow-level logging of all network traffic crossing the Center's network perimeter. The internal (Juniper) firewalls do not currently have a central management server system and are managed as separate individual entities at this time.

Intrusion detection and anomalous traffic identification functions are delivered using a mix of intrusion detection sensor servers running the open source SNORT Intrusion Detection System (IDS) applications/sensors, TCPDump raw packet capture systems, and the legacy ISS Real Secure COTS IDS application. The raw data delivered by these systems is post-capture processed by a series of internally developed Perl scripts and other open source reporting tools. These sensors are located both at the Center's perimeter, as well as spread across the KSC campus backbone networks at key monitoring/transit locations. They are also managed independently of the current NASA Security Operation Center (SOC)

This system also houses some of the Agency Security Operations Center remotely supported intrusion detection and monitoring capabilities based on a variety of COTS software products using Intel-based server platforms that are supported as part of the local NSP infrastructure.

4.8.9.4 Network Operations

Network Operations is supported primarily by the following groups: Design Engineering, Operations Engineering, Platform Engineering, Field System Specialists, and Network Technicians.

The Design Engineers are responsible for design, integration, and testing of sustaining and large upgrade projects. Design Engineers also provides project management of large tasks. Finally, the Design Engineers is responsible for the exploration of new technologies.

The Operations Engineers provide engineering support to day-to-day tasks. Tasks include dispensation of trouble tickets, network administration, network security, and configuration management. The Operations Engineers may also provide operational insights to the Design Engineer's projects.

The Platform Engineers are responsible design, operations, and maintenance of the servers, workstations, and applications that supports KNET. The Platform Engineers, with the support of the Operations Engineers, are mainly responsible for the Network security plans – including Certification and Accreditation.

The Field System Specialists are responsible for the configuration control of the network equipment.

The Network Technicians provide hands-on support for KNET. The Network Technicians are responsible for the operations of the Network Control Center (NCC). Tasks range from day-to-day support to the installation and configuration of new systems.

Some of the applications used to support network operations are described in section 4.8.9.1.

4.8.9.5 Network Processes

KNET uses the IMCS Maximo work order system to process Network trouble tickets and work orders.

Network trouble tickets are typically submitted by telephone to the IMCS Comm. Control. IMCS Comm. Control gathers the information and creates a Maximo Work Order with the

relevant information for the KNET team. In some cases, the local service providers (ODIN, USA, Boeing, etc.) help desk can submit the trouble ticket directly to the NCC. In addition, high profile customers can also submit trouble tickets directly to the NCC. Once the information is entered into the IMCS Maximo system, the NCC leads would assign techs to work the issues.

Network work request are submitted to the IMCS Production Control office where the details are entered into the IMCS Maximo work order system. As part of the work order process, Production Control may determine the priority and the skill level required to complete each task. As the work order process is passed to the Network group, the Network supervisor can reassign the work order to the appropriate group (Design Engineers, Field System Specialist, etc.) to begin the work order process.

In addition to the IMCS/Network work control process, Network also abide by the many internal IMCS, Programs (Shuttle, Constellation, Expendable Launch Vehicle, Space Station, etc.), and Center-wide processes that may impacts Network services.

4.8.9.6 Network Lab

A small number of integration/test/validation environments exist within the KSC networking environment.

The KNET personnel have a network test bed near the KNET Network Control Center where they can test equipment that may have failed in the field. In addition, KNET has a test lab that is shared between NASA IT and IMCS personnel that is used for compatibility/integration testing of any proposed changes to the existing network infrastructure, integration testing with a wide array of IT equipment and technologies, and off-line copies of the existing KSC network infrastructure and services for the validation of any proposed configuration/operating system changes. These labs are both located in the CIF building and staffed as needed by the contractor and NASA IT personnel.

The NASA Network Security Perimeter group also maintains a small laboratory environment in the CIF building, staffed solely by the network security perimeter Engineering/O&M personnel. This lab verifies the compatibility of any proposed changes to the network security perimeter hardware/software (including the firewalls & Virtual Private networking concentrators) prior to introduction into the operational infrastructure. This lab only houses the equipment directly related to the current network security, as well as any proposed small scale configuration changes. Any more extensive testing required is done so via a NASA task order to another IT support contractor at KSC at this time.

4.8.9.7 Hardware Description

The Hardware used in the KSC Local Area Networks is largely Cisco Systems based routers and switches (with a number of legacy 3Com switches), Juniper and Checkpoint NGX Firewalls and Dell server hardware platforms.

A detailed list of the involved hardware is also included in the Hardware inventory Appendix.

4.8.9.8 Hardware Refresh

There are no standard hardware refresh cycles at the Kennedy Space Center due to an on-going lack of adequate funding. Hardware is refreshed when it a) can no longer be supported, b) no longer supports the connectivity requirements it must satisfy and c) funding has been identified and made available for this purpose.

4.8.10 Collaboration Services

The Current KSC networking contractor does not provide any collaboration services. These services are currently provided by the UNITeS contractor as part of the Wide Area Network services.

4.8.11 Customer Relationship Management

The following tables contain network demarcation information and "touch points" to other local area networks at the Center.

External/Perimeter/Off-site/Near-Site

Interface Name	Supporting Organization	Description
45th Space Wing Network	USAF – 45th Space Wing	KSC Interface to 45th Space Wing Network @ Cape Canaveral AFS/Patrick AFB (External)
Boeing Building 100 Corporate Network	Boeing	KSC Interface to Boeing Corporate Network @ near-site facility (External)
KSC Visitor Complex DNC Network	Delaware North Corporation (DNC)	KSC Interface to near-site KSC Visitor Complex DNC Corporate Network (External)
Vandenberg AFB (VAFB)	Expendable Launch Vehicle Integrated Support (ELVIS) Contractor-Analex	KSC Internal Networks Extension to Vandenberg AFB in Lompoc, CA (Internal)
AMF-CSE Network	AMF-CSE	Astronaut Memorial Foundation Center for Space Education – Outreach/ Education network environment inside of the AMF-CSE facility @ the KSC Visitor Complex (Internal)
ASO Open Network	Astrotech Spacecraft Operations	KSC Open Network Extension to near-site

Extension		payload processing facility in Titusville, FL (Perimeter/Internal)
FDLE Network Extension	Florida Dept of Law Enforcement	Stub Network extension of the FDLE network to selected KSC facilities- Air gap
ELV Resident Office-Littleton, CO	Expendable Launch Vehicle Integrated Support (ELVIS) Contractor-Analex	KSC Perimeter Networks Extension to Expendable Launch Vehicle Resident Office (Perimeter/Internal)
ELV Resident Office-Chandler, AZ	Expendable Launch Vehicle Integrated Support (ELVIS) Contractor-Analex	KSC Perimeter Networks Extension to Expendable Launch Vehicle Resident Office (Perimeter/Internal)
ELV Resident Office-Sterling, VA	Expendable Launch Vehicle Integrated Support (ELVIS) Contractor-Analex	KSC Perimeter Networks Extension to Expendable Launch Vehicle Resident Office (Perimeter/Internal)
Telescience & Internet System Lab (TSIL)	NASA IT Directorate	NASA Telescience Lab Network in O&C – Supports NASA Desert RATS activities & Off-site Tunnels (Perimeter/Internal)
ISTEF Network	Computer Sciences Corp (CSC)	Joint Use facility for NASA/USAF Research – Innovative Science & Technology Experiment Facility (Internal)

Internal

Launch Operations Network (LON)	United Space Alliance (USA)-SPOC	Interface to Launch Operations Network environments in the Launch Complex 39 Areas (Internal)
USA Shuttle Data Center - VAB	United Space Alliance (USA) -SPOC	Data Center Network in the Vehicle Assembly Building (Internal)
KSC Advanced Visualization Environments (KAVE)	United Space Alliance (USA) -SPOC	Interface to the KAVE Networks in the VAB & LCC (Internal)
CAPPS CIMS/Data Center – O&C	Boeing (CAPPS)	Checkout, Assembly & Payload Processing Services Data Center Network (CAPPS) in O&C Building (Internal)
CAPPS CIMS/Data Center – SSPF	Boeing (CAPPS)	Checkout, Assembly & Payload Processing Services Data Center Network (CAPPS) - Space Station Processing Facility (Internal)
SRB Network (including SRB Data Center)	United Space Alliance (USA)-SPOC	Legacy Network interconnecting Solid Rocket Booster Processing facilities @ KSC & CCAFS (Internal)
SRB Network -CCAFS	United Space Alliance (USA)-SPOC	SRB Facility Networks in Hgr M& N @ CCAFS (Internal)
Ground Support Eqpt (GSE) Lab	Boeing (CAPPS)	GSE Development environment-(Internal)
Automated Radio Frequency Mgmt System Network (ARFMS)	Boeing (CAPPS)	ElectroMagnetic Lab Network -(Internal)
KSC Complex Control System (KCCS)- Shuttle	United Space Alliance (USA)	Semi-isolated SCADA network providing utilities telemetry/control & Building automation across LC-39 area -(Internal)
ELV Mission Analysis Computer Lab	Expendable Launch Vehicle Integrated Support (ELVIS) Contractor-Analex	Telemetry Analysis Environment managed by ELV contractor (Internal)
PWR Data Center Network	United Technologies-Pratt Whitney Rocketdyne	Data Center Network in the Operations Support Building (OSB) - (Internal)
IRT Acceptance Test Facility	NASA IT Directorate	NASA IT Acceptance Test Facility in CIF Building-(Internal)
LSSC Data Center	Life Science Support Contractor (LSSC)- Dynamac	Data Center Network in the Space Life Sciences Laboratory (SLSL)-(Internal)
CRCA Facility Network	Wiltech (USA Subcontractor)	Network in the Component Refurbishment Chemical Analysis (CRCA) facility

National Park Service (NPS) Network	National Park Service (NPS)	National Park Service (NPS)/Fish & Wildlife Service Networks in the Merritt Island Wildlife Refuge (Internal) -
TCMS	Boeing (CAPPS)	Test Checkout & Management System Network – SSPF (Internal)
LPS Software Development Network (LSDN)	United Space Alliance (USA)	Semi-isolated network for Launch Processing Systems Development (Internal)
Andover Network	Boeing (CAPPS)	Facility Mgmt /Control/Building Automation SCADA network for the SSPF & O&C facilities (Internal)
Distributed Observer Network (DON)	NASA IT	Simulation & Testing Environment in the O&C Building (Internal)
Corrosion Control Test Facility Network	NASA IT	Remote Testing lab environment - (Internal)
Transient Systems Lab Network	NASA IT	IT Lab environment (Internal)
SMA Development Lab	NASA IT	IT Lab environment (Internal)
Collaborative Engineering Environment (CEE)	NASA IT	IT Lab environment (Internal)
Challenger Outreach lab	NASA IT	IT Lab environment (Internal)
Command, Control & Communications Element (CCCE)	NASA NE & USTDC Contractor (ASRC)	Development environment for Next Generation Ground Processing/Control systems (Internal)
Engineering Development Lab (EDE)	NASA NE & USTDC Contractor (ASRC)	Development environment for Engineering Labs (Internal)
BoosterNet	United Space Alliance (USA)	Shuttle Processing Data & checkout environments , includes Automated Booster Assembly Checkout System (ABACS) (Internal)
CCAFS Complex 20 Network	NASA IT	Network Extension to Cape Canaveral AFS Launch Complex 20 facilities

4.8.12 IT Security

IT security planning, implementation, and compliance is integral to all work performed at KSC and, therefore, is the responsibility of the entire contractor workforce. The current contractor is responsible for providing technical support for IT security to the individual system owner, CO, COTR, Organization Computer Security Official (OCSO), Center CIO, Information Assurance Officer (IAO), and Center IT Security Manager (ITSM).

The current contractor develops documents, maintains, and manages operational and technical IT security policies, procedures, and controls for all services that the contractor provides to the Government. For each of these delivered services, the contractor integrates the IT security policies, procedures, and control measures into the supported systems full life cycle. This includes both testing and the annual review of these policies, procedures, and controls for adequacy and compliance.

The contractor is not responsible for providing administrative or engineering desktops, workstations, or laptops for their use in the performance of this contract, as they are Government provided via the Outsourcing Desktop Initiative for NASA (ODIN) contractor or successor. For Government-furnished IT services, the Government is responsible for all necessary actions to achieve IT security compliance for the respective system. For all contractor provided IT systems and GFP that the contractor is responsible for operating and maintaining, the contractor is responsible for ensuring IT security compliance with the applicable .

For each system and service provided by the contractor in performance of this contract, the contractor currently establishes, implements, complies and maintains and implement IT Security Plans in accordance with NPR 2810.1A.

The KSC IT Security function utilizes various tools to help perform vulnerability scanning, incident response and IT Security system review and assessment, including the required documentation.

Vulnerability scanning is performed throughout the month across the entire KSC network environment (including the related remote KSC locations), based on a list of potential vulnerabilities developed by the NASA Security Operation Center. Once the scanning is completed using an Agency standard set of software tools, a series of largely automated reports are compiled, generated, and reviewed prior to dissemination for each organization on the type and severity of the vulnerabilities that were detected on the hosts for which they are responsible. These organizations then report back on the status of vulnerabilities that were identified during the scans and this IT Security function tracks the progress of fully mitigating these vulnerabilities. Initial system scans are required prior to the connection of a new system being to the center's network environment or whenever substantial changes to the IT Security posture are made to existing IT systems.

Incident Response & Computer Security Forensics are often required in support of IT Security event investigations. This function provides technical support to the KSC IT Security Manager is the detection, isolation and remediation of IT Security Incidents and issues.

IT Security plans are submitted to the Government for technical review and assessment. This process follows the approved Agency requirements and procedures for these functions. The KSC IT Security Office reviews every security plan for the required basic content. After this has been completed, IT Security documents, tracks, and performs the initial levels of assessment of the system security plan before starting the formal Agency certification and accreditation process.

KSC utilizes both the McAfee Foundstone IT security vulnerability scanning/reporting tool as well as the Nessus (open source) tool for the detection and identification of IT Security vulnerabilities. Both the Foundstone and Nessus scanners are Government Furnished Equipment and are configured specifically for this activity. Incident response and computer security forensics capabilities utilize the Encase Forensics disk imaging tool. In the future, a standard Agency Incident Response/Forensics toolkit will be deployed, using mostly open source software tools & Agency developed scripts. In the future, there will also be a center standard IT Security Event Management system that will house the raw investigation data, notes, and analysis results for each of the center's potential events and actual IT Security incidents over the course of the investigation and for historical purposes.

4.8.13 Cable Plant Services (RESERVED)

KSC's Cable Plant system is supported by the KSC IMCS contract. Any required Cable plant services are obtained through this contract vehicle.

4.8.14 Emergency Warning System (RESERVED)

KSC's Emergency Warning system (also Referred to as the Paging & Area Warning System (PAWS)) is supported by the KSC IMCS contract. Any required Area Warning System services are obtained through this contract vehicle.

4.8.15 Public Address Systems (RESERVED)

KSC's Public Address system (also Referred to as the Paging & Area Warning System (PAWS)) is supported by the KSC IMCS contract. Any required Cable plant services are obtained through this contract vehicle.

4.8.16 Radio Systems (RESERVED)

KSC's Radio Systems/Services are supported by the KSC IMCS contract. Any required Radio Systems/Services are obtained through this contract vehicle.

4.8.17 Telephone Services (RESERVED)

KSC's Time Division Multiplexing (TDM) Telephone system is supported by the KSC IMCS contract. Any required Telephone Services are obtained through this contract vehicle.

4.8.18 VoIP (RESERVED)

KSC's VoIP Telephone system is supported by the KSC IMCS contract. Any required VoIP telephone services are obtained through this contract vehicle.

4.8.19 Cable Television Systems (RESERVED)

KSC's Cable Television Systems/Services are supported by the KSC IMCS contract. Any required Cable Television Systems/Services are obtained through this contract vehicle.

4.8.20 Continuation of Center Zoned Architecture Project (CZAP)

No funding has yet been identified to complete the required Zoned Architecture modifications necessary to implement this Agency initiative, so no schedule is currently available. It is anticipated that very little of the required transition work will be complete at transition time to this contract due to a lack of adequate identified funding

4.8.21 Ongoing Center-Specific Projects

In any given year, KSC has many site activation tasks. In addition, the Operation and Checkout facility is undergoing a major renovation to refurbish the facility. The last phase is currently scheduled to be completed in FY11, but may slip, depending on funds availability.

KSC is in the process of upgrading facilities and adding network services to support the Constellation program. There are currently anticipated to be a number of installations in support in the FY11- FY13 timeframe, but no specifics currently exist.

4.8.22 Work Load Indicators

	Work Load Indicators	**FY 10/ per mo**	**FY 11/ per mo**	**FY 12/ per mo**	**FY 13/ per mo**	**FY 14/ per mo**	**FY 15/ per mo**	**FY 16/ per mo**	**FY 17/ per mo**
Network Services	Trouble Tickets	N/A	N/A	75	85	90	95	95	100
Network Services	Support Requests	N/A	N/A	75	85	90	95	100	100
Network Security Perimeter	Access Request (i.e. Firewall	N/A	N/A	20	20	20	20	15	15

	Openings/ Mods)								
Network Security Perimeter	Support Requests	N/A	N/A	10	10	10	15	15	20
Secure Remote Access	Custom VPN Support Requests	N/A	N/A	10	10	15	20	25	30

4.8.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

Located at Executive Orders:
(http://www.archives.gov/federal-register/executive-orders/)

a. Executive Order EO13423, Strengthening Federal Environmental, Energy, and Transportation Management

Located at: NASA Standards: http://standards.nasa.gov

a. NASA-STD-8719.9, Standard for Lifting Devices and Equipment.

Located at NODIS: (http://nodis3.gsfc.nasa.gov)

a. NPD 6000.1, *Transportation Management*
b. NPR 6200.1, *NASA Transportation and General Traffic Management*
c. NPR 8621.1, *NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping*
d. NPD 8710.5, *NASA Safety Policy for Pressure Vessels and Pressurized Systems*
e. NPR 8715.3B, *NASA General Safety Program Requirements*

Located at the NFS:
(http://www.hq.nasa.gov/office/procurement/regs/nfstocA.htm)

a. NFS 1852.223-70, *Safety and Health*
b. NFS 1852.223-73, *Safety and Health Plan*

4.9 LANGELY RESEARCH CENTER (LARC)

Langley Research Center (LaRC) is located adjacent to Langley Air Force Base in Hampton, Virginia. LaRC supports approximately 4,000 users and approximately 10,000 network devices. These devices are dispersed between approximately 100 individual campus buildings that require LaRC network services. The LaRC network infrastructure consists of about 650 devices. Customer requests for LaRC network services must be submitted in accordance with LMS-CP-5519 and LMS-CP-5521.

4.9.1 Property/Inventory

Government-tagged equipment is managed by NASA property custodians using the Agency's N-PROP system. The contractor will be listed as the user of the equipment and provide updates to the physical location the equipment. The physical control and configuration of all equipment, including non-controlled equipment, is managed by the contractor in accordance with LMS-CP-2716.

4.9.2 Shipping/Receiving/Inspection

All deliveries must go to Building 1206 at 4 South Marvin Street for inspection before final delivery. All delivery vehicles must first stop at the main gate for inspection. The driver and any passengers must also have a visitor badge to enter the Center. Shipments can also be handled by Building 1206, however, shipment of any controlled (e.g., government tagged equipment) must be accompanied by a completed LF 52 – Shipping/Transfer Document.

4.9.3 Vehicles Necessary To Support Center Work

Under the current contract, 6 vans are provided by the contractor to support operations that would be in-scope of the NICS contract. The cable plant staff has 3 vans, the network staff has 1 van, the telecomm staff has 1 van and the video distribution staff has 1 van.

4.9.4 Physical Security

All communications facilities and closets have access limited by badge, cipher-lock or key-lock.

4.9.5 Emergency Management

The LaRC Emergency Operations Center (EOC) is currently located in Building 1248 at 10 Langley Boulevard, but may be established elsewhere if the situation warrants. The Center CIO is the Primary Point of Contact (POC) to the EOC for IT-related requirements. In the event the Primary POC is not available, the COOP succession plan is consulted to identify the next OCIO POC. The Center CIO will coordinates with the ODIN contractor POCs using the contractor's call down list as necessary.

4.9.5.1 Center Specific COOP Support

The Center maintains a Continuity of Operations (COOP) plan. This plan is considered Sensitive But Unclassified (SBU) and is not publicly-available. The Center CIO coordinates any COOP requests with the ODIN contractor.

4.9.5.2 Service Continuity of Operations Support

The ODIN contractor maintains a communications services COOP plan. This plan is considered SBU and is not publicly-available.

4.9.6 Safety

Center safety policies and procedures will be adhered to.

4.9.7 Facilities

Building	Room Number	Room Type - Subtype	Net Square Feet
641	150	Network/Phone Switch Equipment	273
641	151	UPS System Equipment	85
Total			358
Building	Room Number	Room Type - Subtype	Net Square Feet
1201	1	Storage	101
1201	101	Office	94
1201	102	Office	169
1201	103	Office	129
1201	104	Office	150
1201	105	Office	319
1201	106	Office	241
1201	112	Telephone Switch Equipment	1452
1201	113	UPS System Equipment	237
1201	115A	ViTS Room	432

1201	115B	ViTS Equipment	251
1201	115C	Communication Demarks (e.g., Verizon, FTS, Lambda)	463
1201	115D	Video Head End	343
1201	116	Storage	210
1201	117	Storage	683
1201	118	Office	1295
1201	119	Storage	56
Total			6625
Building	Room Number	Room Type - Subtype	Net Square Feet
1211	100	Network/Phone Switch Equipment	1047
1211	101	UPS System Equipment	214
Total			1261
Building	Room Number	Room Type - Subtype	Net Square Feet
1213	139	NISN OFFICES	423
1213	144	NISN Networking Equipment	1290
1213	144A	NISN UPS System	183
1213	144B	NISN Storage	208
Total			2104
Building	Room Number	Room Type - Subtype	Net Square Feet
1268	2092	Office	1183
1268A	1105	Core Networking Equipment	611
1268A	1105A	Network Operations Center	402
1268B	2212	Office	313
1268B	2215	Network Lab	1110
1268B	2218	Office	273

Totals			3892
Grand Total			14240

4.9.8 Network Services

Basic Network Services are Domain Name Service (DNS) resolution, Dynamic Host Configuration Protocol (DHCP), Remote Access Service (RAS), Network Time Protocol (NTP) and Guest Network Service.

4.9.8.1 IPAM

DNS resolves IP hostnames to IP addresses and is provided by centrally managed Agency DNS servers. Local Network Operations staff provides daily updates to the DNS database. DHCP allows network devices to be automatically configured using a central database and is provided by centrally managed Agency DHCP servers. The Local Network Operations staff provides daily updates to the DHCP database.

4.9.8.2 RAS

The Langley Remote Access system (LaRA) system allows remote devices to dial-into the campus. Since the system is considered external, users must also use the Center VPN system to gain access to internal Center resources. VPN requests are handled in accordance with LMS-CP-5915.

4.9.8.3 NTP

NTP provides a mechanism where all system clocks may be synchronized and is provided from within LaRCNET.

4.9.8.4 Guest Network

The Langley Public Wireless and Guest Network (WaGN) is designed to provide wired and wireless connectivity for official LaRC guests at various conference rooms throughout the Langley campus. Permanent Langley employees may use this service through a wireless connection at the same locations.

a) Wireless Guests

Guest access will be granted to temporary visitors for up to 10 working days at no charge. If access is needed beyond this period of time, the sponsoring organization must purchase an ODIN seat to support the usage. Wireless client systems must be Wi-Fi compliant and must utilize IEEE 802.11b and 802.11g standards. These clients must be based on the Internet

Protocol (IP). Wireless users must utilize the Service Set Identifier (SSID) obtained from ODIN and properly configure the SSID on their computer system. The system must also be configured to obtain an IP address, default gateway, and domain name service automatically using Dynamic Host Configuration Protocol (DHCP).

b) Wired Guests

Guests may use a designated jack for a wired connection to the Public Wireless and Guest Network if a Langley organization has purchased a seat to support that connection. Public Wireless and Guest Network jacks are color-coded yellow. Wired users must configure their computer system to obtain an IP address, default gateway, and domain name service automatically using DHCP.

4.9.9 Data Services

The purpose of LaRCNET is to interconnect the Langley's IT systems with each other and to support communications with external systems through connections with wide area network service providers, NISN and NREN. LaRCNET provides a communications medium through which NASA scientists, engineers, researchers, and support staff can share information quickly and efficiently. By providing this service, LaRCNET enables LaRC to support NASA missions.

4.9.9.1 High Level LAN Description

LaRCNET is the LaRC centrally managed local area network. LaRCNET Network Infrastructure is comprised of the cable plant, electronics, and programs needed to transport the data of Center IT systems. The Network Infrastructure utilizes Ethernet switches that interconnect using Category 5e twisted pair or fiber optic cabling. The primary network protocol is Internet Protocol (IP), and IP routing services are provided to allow intra-campus communications as well as external communications.

The Network Infrastructure has two logical sections, which are referred to as Internal and External LaRCNET.

Internal LaRCNET supports the majority of network connections. The Internal LaRCNET backbone connects to various networks including device access networks, management networks, wind tunnel networks, and special project networks. The backbone joins the 100+ building/distribution networks that make up LaRCNET. All of the buildings that connect to the backbone have Ethernet segments that run throughout the building. TCP/IP and UDP/IP are the main protocols supported across the backbone. The access networks connect most of the 10,000+ devices on LaRCNET, using 10/100/1000 Mbps Ethernet. The Center firewall system defines the outer-most part of Internal LaRCNET.

External LaRCNET is composed of several networks including De-Militarized Zones (DMZs), The Wireless and Guest Network (WaGN), The Isolation Network, and the Langley Remote Access system (LaRA).

The DMZs provide restricted and isolated access to services that are available to communities outside of Langley. They also provide protective services to the Center's client-to-network Virtual Private Network (VPN) server. The DMZs utilize 100 Mbps Ethernet and are restricted to TCP/IP services.

DMZ-A is a DMZ network that connects devices that provide IT Security and Network services. The devices on DMZ-A are managed by ITIB. Services on DMZ-A include external client-VPN concentrator, RSA two-factor authentication server, etc. Along with custom firewall rules, the following general logic applies to DMZ-A:

a) Outside Network devices are allowed to initiate connections to DMZ-A devices.
b) Internal LaRCNet devices are allowed to initiate connections to DMZ-A devices.
c) DMZ-A devices are not allowed to initiate connections to Outside Network devices.
d) DMZ-A devices are not generally allowed to initiate connections to Internal LaRCNet devices.

DMZ-B is a DMZ network that connects devices that provide services on behalf of non-OCIO Langley projects. The devices on DMZ-B are managed by non-OCIO organizations. Along with custom firewall rules, the following general logic applies to DMZ-B:

a) Outside Network devices are allowed to initiate connections to DMZ-B devices.
b) Internal LaRCNet devices are allowed to initiate connections to DMZ-B devices.
c) DMZ-B devices are not allowed to initiate connections to Outside Network devices.
d) DMZ-B devices are not generally allowed to initiate connections to Internal LaRCNet devices.

DMZ-C is a DMZ network that connects devices that provide services on behalf of the Langley OCIO and Agency projects. The devices on DMZ-C are managed by the OCIO. Services on DMZ-C include NX, WIMS, Center web servers, and ePayroll. Along with custom firewall rules, the following general logic applies to DMZ-C:

a) Outside Network devices are allowed to initiate connections to DMZ-C devices.
b) Internal LaRCNet devices are allowed to initiate connections to DMZ-C devices.
c) DMZ-C devices are not allowed to initiate connections to Outside Network devices.
d) DMZ-C devices are not generally allowed to initiate connections to Internal LaRCNet devices.

DMZ-D is a DMZ network that connects devices that provide services on behalf of non-OCIO Langley projects. DMZ-D differs from DMZ-B in that the server configurations use ports and protocols that create a high security risk to the servers and other systems. DMZ-D devices are managed by non-OCIO organizations. Along with custom firewall rules, the following general logic applies to DMZ-D:

a) Outside Network devices are allowed to initiate connections to DMZ-D devices.
b) Internal LaRCNet devices are allowed to initiate connections to DMZ-D devices.
c) DMZ-D devices are allowed to initiate connections to Outside Networks devices.
d) DMZ-D devices are not generally allowed to initiate connections to Internal LaRCNet devices.

The Wireless and Guest Network (WaGN) utilizes the same cable plant as LaRCNET, but uses separate electronics and control infrastructure. It provides less restrictive network access for guests and visitors, as well as access for projects whose network requirements demand more open accessibility than that available on Internal LaRCNET.

The Isolation Network supports all of Langley's connections to other NASA locations and to non-NASA networks, including the Internet. The network utilizes a high performance routing switch to interconnect the Center's firewall system to the NISN Standard and Premium services and to the NREN. Through NISN, Langley users can access the Internet.

4.9.9.2 Wireless Networks

Permanent Langley employees will only connect to the Langley Public Wireless and Guest Network through a device that has a registered ODIN seat associated with it. Guest access will be granted to temporary visitors for up to 10 working days at no charge. If access is needed beyond this period of time, the sponsoring organization must purchase an ODIN seat to support the usage. Wireless client systems must be Wi-Fi compliant and must utilize IEEE 802.11b and 802.11g standards. These clients must be based on the Internet Protocol, IP. Wireless users must utilize the Service Set Identifier (SSID) obtained from ODIN and properly configure the SSID on their computer system. The system must also be configured to obtain an IP address, default gateway, and domain name service automatically using Dynamic Host Configuration Protocol (DHCP). Management of Langley’s wireless network is in accordance with LPR 2570.5.

4.9.9.3 Network Security

The Security Architecture defines the Langley Center and Public Firewalls, as well as the Center VPN systems, which reside at the border of the Langley network providing perimeter protection. At the border and internally, Intrusion Detection and Monitoring devices are in place along with an Incident Response and Computer Forensics capability. The Langley internal network is segmented utilizing managed internal firewalls. These firewalls typically segment backend

networks that support the NASA Wind Tunnels and other specialized networks. All Langley firewalls are centrally managed and monitored by IT Security operations. Currently there are seven intranet firewall systems. Firewall rules requests are processed in accordance with LMS-CP-5696.

4.9.9.4 Network Operations

The local Langley Network Operations Center (NOC) is located in building 1268 and provides displays for network management/monitoring hardware. The local NOC is the second-tier resource for the central ODIN/LARC Help Desk. The NOC supports seating for approximately five personnel. Tasks performed by the local NOC include:

a) Dispatch Net Ops analysts/engineers, or Network Cable Plant personnel when appropriate
b) Track and follow up on ALL network-related Remedy trouble tickets
c) Central point of contact and coordination for all LaRCNET-related network issues
d) Real-time monitoring and authoritative source of network status
e) Monitor Post Office server performance and usage/traffic volume
f) Email user account administration
g) LaRA remote access user account administration
h) Email and LaRA account password resets
i) Real-time monitoring of key network infrastructure devices
j) On-line network traffic flow monitoring
k) Preliminary LaRCNET troubleshooting
l) Generate and distribute facility power outage notifications
m) Update the LaRCNET and Provance databases when changes are appropriate
n) Investigate and correct IP address and host name conflicts
o) Partition and re-enable network connections as required to resolve network issues and/or facilitate the correction of non-compliant or vulnerable systems as identified by IT Security

Network Management is supported in the form of configuration management and monitoring. A collection of commercial off-the-shelf and open-source applications are used to manage and monitor the Network Infrastructure and Basic Network Services.

The Network Management devices are used to manage and monitor the Network Infrastructure. Vendor specific applications are used to provide most of the configuration management and monitoring functions. Additional monitoring is accomplished through the use of open-source and locally developed tools that use the Simple Network Management Protocol (SNMP).

Devices are managed remotely using remote terminal sessions or SNMP. A management network utilizes virtual LAN technology to logically segregate the network control traffic from the user system traffic. The current software tools include:

a) Orion Solarwinds and ARGUS for network polling and alert generation
b) MRTG for network performance and trend analysis
c) CiscoWorks LMS for network management and visual alerting
d) Cisco ACS for access control to the network infrastructure and management tools
e) TCPDump and Network Instruments Observers for traffic capture and analysis
f) BBSM for monitoring and control of access to the wireless infrastructure

4.9.9.5 Network Processes

Major configuration and change management for the network infrastructure is governed by the Langley Network Configuration Control board. This board is governed by the Langley CIO and manages the configuration for the entire Langley IT infrastructure. Moves, adds, and changes to the network infrastructure are reflected within the network management tools described above and in network drawings. Trouble tickets are generated by a central enterprise help desk and those directed to Langley are placed in an appropriate queue which is monitored by a local helpdesk. The queues include Network Operations, Server Operations, Cable Plant Service, IT Security, and Desktop Services. The monthly average for tickets for Network Operations issues is approximately 50 trouble tickets.

4.9.9.6 Network Lab

Langley has a network lab created to support integration and upgrade testing. The Langley network lab consists of replicas of several Langley core, distribution, and access switches, wireless infrastructure, remote access infrastructure, and DNS service. The configuration of the lab changes as needed for testing. The network lab also houses a SmartBits network performance analysis system which allows testing, analysis, and certification of network equipment configuration and function prior to placement in production. All new hardware platforms and operating system versions are tested in this lab environment prior to placement into production.

4.9.9.7 Hardware Description

The following hardware platforms and software platforms are utilized to create LaRC Network and IT Security Architecture.

Qty	Make & Model	Function
14	Cisco 6509	Core and Distribution points within the LaRC campus network

Qty	Make & Model	Function
	Multilayer Switches	
1	Cisco 6506 Multilayer Switch	Distribution point within the LaRC campus network
10	Cisco CEF 720	Supervisor Blades
9	Cisco Sup 2	Supervisor Blades
1	Cisco Sup 32	Supervisor Blade
49	Cisco 4006	Distribution and Access Layer devices within the LaRC campus network
2	Cisco 4006	Public Wireless Distribution Layer devices
46	Cisco 4506	Distribution and Access Layer devices within the LaRC campus network
11	Cisco 3550 Switches	Access Layer devices within the LaRC campus network
28	Cisco 3550 Switches	Public Wireless Access and Distribution Layer devices
2	Cisco 3560G Switches	Public Wireless Access Layer devices
2	Cisco 3560E Switches	10Gig devices
66	Cisco 3750 Switches	Access Layer devices on the LaRC campus network
12	Cisco 3750 Switches	Public Wireless Access and Distribution Layer devices
5	Cisco 3548 Switches	Access Layer devices within the LaRC campus network
7	Cisco 2950 Switches	Access Layer devices within the LaRC campus network

Qty	Make & Model	Function
85	Cisco 2950 Switches	Public Wireless Access and Distribution Layer devices
3	Cisco BBSM	Wireless LAN management System
1	Cisco WLSE	Wireless LAN management System
44	Cisco 1242	Managed Wireless Access Points
127	Cisco 1200	Managed Wireless Access Points
4	Cisco 2621	Routers
4	Cisco 2924	Access Layer devices on the LaRC campus network
22	Cisco 2960	Public Wireless Access Layer devices
2	Cisco 2970	Public Wireless Access Layer devices
3	Cisco 2970	SPAN switches for network monitoring
1	Cisco AS5300	Remote Access Server
11	IBM CIEGSM	Blade Center
2	Sun T5140	CiscoWorks LMS for Network Management
2	HP DL 380	Cisco Access Control Server for Authentication to Access Network Devices
4	Dell Server-CentOS	TCPDump Network Analyzers
18	Network Instrument Observers	Network Analyzers
3	HP DL 580 Server and HP DL 380	Orion Solarwinds Network Monitoring and Trend Analysis
3	Compaq DL	Windows 2003 Domain Controllers
4	Sun Ultra 450	Tivoli Backup Servers
5	Compaq DL	MS SQL, IIS, Cluster Servers

Qty	Make & Model	Function
2	ALR	Windows NT 4 Server - Communications Tracking System
1	Compaq DL	Windows NT 4 - Web Development Server
1	HP DL 380	Windows 2000 System Management Servers
3	8e6 R3000G Web Filter	Linux based appliance
2	8e6 Reporter Log Server	Linux based appliance
1	HP Windows Server	HP Server for Blocked Pages
1	Cisco 3015	VPN Concentrator
2	Juniper	SSL VPN Concentrator
1	Sun/Solaris	RSA Servers
4	Cisco PIX 535	Center and EOS ANGe Firewalls
4	Cisco PIX 525	Public Network Firewall
3	Cisco PIX 515E	Special Project Firewalls
7	SuperMicro-CentOS	Intrusion Detection Systems (Snort)
2	SuperMicro-CentOS	Nessus Scanner
1	Dell Poweredge 2850-Red Hat	Intellitactics Data Acquisition/Data Warehouse (Analysis of Snort Data)
4	SuperMicro-FreeBSD	TCPDump Network Analyzers
2	Dell-CentOS	TCPDump Network Analyzers
2	Dell Poweredge 2850-Red Hat	SQL Database Servers
2	Windows 2003	PatchLink Servers

4.9.9.8 Hardware Refresh

The network electronics hardware refresh cycle at Langley is approximately 5 years with roughly 1/5 of the infrastructure replaced each year.

4.9.10 Collaboration Services

Langley has 4 full-service ViTS rooms located in 4 buildings. These full-service ViTS rooms are all under NISN maintenance and with three of the rooms staffed (operated) by ODIN personnel. Langley has 10 "roll about" ViTS systems, 7 of which are under NISN maintenance. Langley also has 2 "desktop" ViTS systems, neither of which is under NISN maintenance.

4.9.11 Customer Relationship Management

The Center ODIN Delivery Order Contracting Officer's Technical Representative, along with ODIN contractor outreach personnel and IT Infrastructure Branch technical monitors, work with organizational ODIN POC representatives from around the Center to communicate upcoming changes, gathering of new requirements, and soliciting feedback from the customers.

4.9.12 IT Security

The ODIN contractor supports the local Center ITSM as required. Support includes network monitoring and the provision of system logs (e.g., firewall logs, web filtering logs, etc.). The Center ITSM has a separate task to provide support in the investigation of end-user systems in accordance with LMS-CP-5549, LPR 1620.1, and LAPD 2810.1.

4.9.13 Cable Plant Service

The Langley cable plant is composed of a data infrastructure and a telephony infrastructure. The telephony cable plant is described in the telephone section. The data network infrastructure is a standard core, distribution and access model. Approximately 25% of the communications closets have working UPS systems to provide temporary backup power.

4.9.13.1 Optical Fiber

The distribution switches are connected to the core switches via single mode fiber located in underground duct banks that traverse steam tunnels or 4" conduit that interconnect approximately 100 buildings. Distribution and access switches are located in approximately 180 communications closets and are generally interconnected with single mode fiber.

4.9.13.2 Twisted Pair Copper Cabling

Nodes are connected to the access switches using CAT-5e copper cable. There are approximately 8 minor facilities that are connected via copper T-1 connections.

4.9.14 Emergency Warning Systems (RESERVED)

4.9.15 Public Address Systems (RESERVED)

4.9.16 Radio Services (RESERVED)

4.9.17 Telephone Services

Langley Telephone System (LaTS)

4.9.17.1 System Overview

Langley is in the middle of a telephone system upgrade that will be completed by end of FY09. The current LaRC phone system uses a Siemens 9751 Model 70 running 9004.4.38 software and has 13 CBX (computerized branch exchange) Nodes located in 3 switch rooms. Building 1201 has eight Nodes, building 1211 has four Nodes and 641 one Node. The LaRC system has installed hardware capable of handling 8368 Rolmphone devices (devices can be: digital phones, voicemail channels and data lines), 1824 analog lines, 136 analog DID ports, 192 ground start/loop start trunks and 8 T1 spans. Each one of the 13 Nodes is connected to every other Node by twin-ax cable or 62.5 micron multi mode fiber. The twin-ax is used in co-located Nodes and the fiber is used to connect Nodes in other switch rooms. These fiber connections provide redundant voice and data paths for the whole system.

The LaRC telephone system is currently configured with 3,677 digital Rolmphone model 120 telephones, 1,283 digital Rolmphone model 240 speakerphones and 467 digital Rolmphone model 400 display phones. Also configured are 1,325 analog lines used for fax machines, modems, bells, paging, secure telephones and music-on-hold. NASA LARC personnel receive and place 80,000 to 83,000 calls per week. Requests for new services are processed in accordance with LMS-CP-5541 and LAPD 2540.1.

4.9.17.2 Replacement Phone System

LaTS has been in service for nearly 20 years now and is at the end of its useful service life. The NASA Langley OCIO staff has initiated a project to replace the current system with a modern hybrid telephone switch capable of working in the current Langley environment while providing the capability to support newer technologies such as VoIP as the outlying infrastructure is upgraded.

The replacement telephone system is based upon the Nortel CS 1000M IP PBX platform. The platform is a converged hybrid communication solution capable of supporting up to 16,000 telephones – a mixture of Digital/Analog/IP Stations. With the CS 1000M, call and connection-management is distributed, switching is packet-based, cabling is simplified, management of voice and data is unified, and user access is flexible in terms of type of device and location. The CS 1000M's flexible, modular architecture allows Langley to implement IP Telephony in a gradual phased-migration approach based upon business case decisions in the future. The CS 1000 provides full Call Server redundancy to ensure high availability.

The replacement telephone system will support all of the current LaTS features while providing additional benefits particularly in the area of unified messaging.

4.9.17.3 Handsets

The LaRC telephone system is currently configured with 3,677 digital Rolmphone model 120 telephones, 1,283 digital Rolmphone model 240 speakerphones and 467 digital Rolmphone model 400 display phones. Station Features include the following:

a) Auto Intercom
b) Bad Line Reporting
c) Camp
d) Com Groups
e) Conference
f) Connect
g) Do Not Disturb
h) Forwarding
i) Group Pick
j) Hold
k) Park
l) Pick
m) Private Call
n) Repeat dial
o) Save and Repeat Number Dialing
p) Station Speed Dialing
q) System Speed
r) Transfer

4.9.17.4 Voice Mail Services

The Center's voicemail is integrated with the CBX and consists of 6 Networked Nodes of Phonemail with a total of 96 voice channels. The Phonemail system can provide Call Processing functions as well as individual mailboxes for users. The LaRC Phonemail system currently has 4,044 profiles (mailboxes) and 78 call processing profiles. Phonemail Features include the following:

a) Transfers out of the PhoneMail system to the PBX
b) Transfer to name or extension
c) Transfer to the referral extension
d) Transfer to message sender
e) Transfer to the operator
f) Transfer to any extension.
g) Automatic telephone answering
h) Telephone answering with an automatic personal greeting
i) Multiple personal greetings
j) Name/extension identification in the message header

4.9.17.5 E911 Services

While enhanced 911 services are not available on the legacy Rolm system, it will be available on the new Nortel replacement system.

4.9.17.6 Trunks

The demarcation point for local and long distance services is in Building 1201. Verizon is the local service provider. We have 92 DID trunks (in 4 PRI circuits), 115 Central Office trunks (in 5 PRI circuits) and 3 FTS T1 circuits providing 72 long distance trunks.

4.9.18 Voice over Internet Protocol (VoIP)

Included in the Langley telephone system replacement (above) is a VoIP pilot project of approximately 100 VoIP handsets. Additional migration to VoIP will be determined using business case decisions based upon network infrastructure readiness (e.g., network UPS systems, PoE, redundancy, etc.), new construction, building rehab, etc.

4.9.19 Cable Television Services

Langley currently distributes 14 analog channels and 17 digital (QAM) channels over a standard coaxial distribution infrastructure delivering service to 414 drops in 109 buildings. There is also a limited cable television distribution infrastructure that provides local Cox analog cable TV service to 28 drops in 6 buildings.

4.9.20 Continuation of Center Zoned Architecture Project (CZAP)

The Langley CZAP focuses on making the necessary modifications to comply with the NASA's network zone architecture, NCI. In coordination with I^3P, each NASA Center Chief Information Officer (CIO) completed a center impact assessment outlining the tasks necessary to prepare for the transition of their local area networks to the NCI enterprise infrastructure.

Langley is planning to transition from the current network architecture and end network nodes to conform to the Agency security zone architecture as described in the NCI document "NASA Network Architecture Approach, October 2008." It is assumed that a majority of the devices in DMZ-B and DMZ-C (~100 devices) will migrate to the Extranet: Server and Public: Server networks. It is estimated that an additional 400 devices will migrate to either the Intranet, Extranet, or Public Server zones. In some cases, additional hardware will be required to facilitate the transition of servers, particularly servers that currently service public and partner customers with a single interface.

The number of Intranet user network devices is assumed to consist mostly of ODIN fully managed seats. The initial data from the 'All ODIN' transition activity estimates this number to be about 2,500 devices. About 500 devices are assumed to be printer or similar devices that will be located on the Intranet: User zone. It is assumed that the majority of the remaining hosts will not qualify to be located on the Intranet zone, and, therefore, will be located on the Extranet: Autonomous zone. This is approximately 4,500 hosts on the Extranet: Autonomous zone, which will be the majority of the end device connections at Langley.

VLAN segregation of zones is acceptable to both the NCI Project and the Langley CIO. The NCI border architecture must be used for all layer 3 (OSI model) flows between security zones. As a result of this high level analysis, Langley will build a core and distribution network to support the approximately 3,000 connection Intranet and will re-utilize the two current core and distribution networks to support the Extranet and Public zones. The table below summarizes the re-designation of current infrastructure to map into the new security zone architecture.

LAN ZONE INFRASTRUCTURE	PREVIOUS DESIGNATION
LaRCNet Intranet	New
LaRCNet Extranet	Internal LaRCNet
LaRCNet Public	External LaRCNet

The newly designated LaRCNet infrastructure will connect with the Agency managed Center border network for external and inter-zone communications.

4.9.21 Ongoing Center-Specific Projects

4.9.21.1 LaRC New Town Concept Project

The majority of Langley's research facilities and infrastructure were constructed in the 1950s and early 1960s, and today require significant investment to upgrade and sustain them in reliable working order. As the building inventory approaches 50 years-old, there are increasing demands for maintenance and upgrades.

In order to recapture the operational integrity of the facilities, and reverse the declining trend in its Facilities Condition Index (FCI), Langley has initiated a targeted program of "repair by replacement". The pool of facilities identified as most needing attention are collectively referred as the "Prototype", and the implementation of the targeted program is the Center's "New Town" concept.

Through a methodical evaluation of building investment indicators and redevelopment cost factors, a facility Prototype has been identified that represents a combination of new and renovated facilities that will provide a new core of flexible, state-of-the-art facilities to support Langley's evolving mission. Implementation of the Prototype will allow the Center to improve its Facilities Condition Index score, while reducing its overall building area and required campus footprint. It will also reduce the high annual maintenance and operational burden on the Center, a savings that can be passed on to each program group using Langley's facilities.

Implementation of the Prototype will require an investment exceeding $100 million (Net Present Value), which can be phased. (This investment represents almost $100 million for design and construction, plus additional costs for furniture, communications, etc.) The Prototype will impact approximately 16% of the existing campus through new construction and renovation of approximately 440,000 sq ft. Through the efficiencies gained in this program, this 440,000 sq ft will actually replace 575,000 sq ft of existing facilities. The New Town project is comprised of 6 phases. Phase I, which includes the design and construction of Administrative Office Building 1 began Q1 of FY09, and is scheduled for completion Q1 of FY11.

4.9.22 Work Load Indicators

PWS Section	Indicator	Approximate Quantities/month
3.1.1	IPAM data updates	300 (DHCP), 225 (DNS)

3.1.2	New or updated remote access accounts	40*
3.1.4	Number of guest accounts	3500
3.6	Network trouble tickets	70
3.6	Network moves, adds, changes	1075
3.6	Network service requests	330
3.12	IT security incident response support	2
3.12	Firewall rule changes	20
3.12	Security documentation packages	2
4.9.5	Telephone trouble tickets	70
4.9.5	Telephone moves, adds, changes	850
4.9.5	Telephone service requests	70
5.0	Network projects greater than $500K	1/yearly
*	Only RSA Token/VPN Accounts. This average number is elevated due to WebTADS becoming restricted to NASA networks.	

4.9.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.10 MARSHALL SPACE FLIGHT CENTER (MSFC)

MSFC is responsible for the maintenance and operations of three LANs; the MSFC campus LAN; the National Space Science and Technology Center (NSSTC) located in Huntsville, Alabama; and the Michoud Assembly Facility near New Orleans, Louisiana. Efforts have been made to bring consistency between these three LANs, however each currently operates independently and each has unique background and historical information. A brief description of MSFC three LANs is as follows:

a) MSFC LAN Overview – Network scheduling, network monitoring, network control and system management, problem management, LAN engineering support, LAN operational support is provided by the ODIN contract. The LAN supports over 120 buildings onsite at MSFC. There are approximately 280 communications wiring closets, 390 switches, 14,000 switch ports, 30,000 Cat5/Cat6 circuits, and 600 wireless access points a maintained by the contractor. Additionally, the MSFC LAN extends to a few locations off-site in the Huntsville/Decatur area. Those locations are typically connected via traditional T-1/T-3 circuits, metro Ethernet circuits, or leased dark fiber.

b) MAF LAN Overview - Network scheduling, network monitoring, network control and system management, problem management, LAN engineering support, LAN operational support is provided by the UNITeS contract. The MAF LAN supports over 35 buildings on the MAF campus and provides full wireless coverage to the campus. The LAN consists of approximately 2250 network ports and 275 wireless radios. The majority of the MLAN has been installed in the past few years and utilizes Cat5/Cat6 copper and fiber optic cabling. The MAF IT environment is rapidly changing and will likely remain in such a state of flux for the next few years. The primary driver for the changing environment is the facilities work is migrating from the manufacturing of Shuttle External Tanks (ET) to components for the Constellation Program. As a result two LANs currently support the MAF users, the ET LAN supporting ET requirement and the MLAN supporting all other NASA requirements on campus. The ET LAN is supported and operated by the ET manufacturing contractor, Lockheed Martin, and will remain so until Shuttle Fly-out currently scheduled for FY2010. Due to the soon approaching decommissioning of the ET LAN it is not part of the NICS contract. The MLAN will be part of the NICS contract and will be the only NASA support LAN at the MAF upon ET LAN decommissioning.

c) NSSTC LAN - Network scheduling, network monitoring, network control and system management, problem management, LAN engineering support, LAN operational support is provided by the UNITeS contract. The NSSTC IT environment must maintain logical separation for the IT Services of a multi-tenant environment. As a result multiple VLANs currently support the NSSTC users, the Research University environment and all

other NASA requirements on campus. The NSSTC LAN is installed in a single multistory building with approximately 600 users. The LAN does provide connectivity for the VoIP telephone system, which is the primary telephone system in the facility. Note: the VoIP system is not part of the NICS procurement.

4.10.1 Property/Inventory

The ODIN contractor is considered offsite accountable for all property and inventory items. The UNITeS contractor is considered onsite accountable for all property and inventory.

4.10.2 Shipping/Receiving/Inspection

All shipping, receiving, and inspection for the MSFC LAN is conducted by the ODIN contractor at the ODIN provided warehouse. Equipment is transported on or off center as required. All equipment is tracked by asset tags per applicable policies.

All shipping, receiving, and inspection for the MAF and NSSTC LANs are conducted by the UNITeS contractor at MSFC. Equipment is transported to the appropriate point of use, MAF or NSSTC, as required. All equipment is tracked by asset tags per applicable policies.

4.10.3 Vehicles Necessary to Support Center Work

In support of the MSFC LAN ODIN provides 4 full size work vans for network technicians. In support of the MLAN a government furnished cart is provided. In support of the NSSTC LAN no vehicles are utilized.

4.10.4 Physical Security

In most instances physical security is provided by MSFC Protective Services. Most frequently this security is if the form of electronic badge readers that allow access for authorized personnel to communication rooms. Some communications rooms and equipment locations are still controlled by physical keys and key accountability is the responsibly of the LAN contractor (ODIN and UNITeS) per MSFC policies. The contractor is also accountable for equipment cabinet and other miscellaneous keys.

4.10.5 Emergency Management

4.10.5.1 Center Specific COOP Support

The MSFC LAN works with the MSFC COOP team and depending on the COOP location may provide LAN connectivity during a COOP event. The MAF LAN works with the MAF emergency management team and provides LAN services to the on-site Emergency Operation Center when activated.

4.10.5.2 Service Continuity of Operations Support

The MSFC LAN has been designed to be as resistive to operational impacts as possible to emergency events. However, in the event that critical LAN components are non-operational or unavailable the MSFC LAN contractor has critical LAN components spared in an off-site nearby facility and agreements are in place with manufactures in the event emergency replacements are required.

The MAF campus has recently had significant efforts completed to harden the infrastructure. Most of the IT related hardening projects, such as the cable plant and mobile communications vehicles, will be maintained outside of this contract.

4.10.6 Safety

Both ODIN and UNITeS follow all NASA Agency and Center safety policies and procedures. Both contracts have a person that is responsible for all aspects of safety (LAN and other contract services). Some of the LAN related may require specialized safety training such as elevated work platform training or confined work area training.

4.10.7 Facilities

In support of the MSFC campus LAN the following on-site space is provided to ODIN by NASA.

Provider	Location	Amount	Type	Description
NASA	B4207, Rm 103	550 Sq Ft	Office	Network Management Center
NASA	B4646,2nd Floor	486 Sq Ft	Office	Data Technicians
NASA	B4207, Rm 140		Shared Equipment	Communications Room
NASA	B4207,Rm 145B		Shared Equipment	Communications Room
NASA	B4663,Rm M211		Shared Equipment	Communications Room
NASA	Various across campus	280 rooms	Shared Equipment	Small Communications rooms for Access Layer devices
ODIN	Madison	1000 sq ft	Office	Engineering, Management, and Business offices
ODIN	Madison/ Intergraph	1200 sq ft	Warehouse	Equipment storage

ODIN	Madison/ Intergraph	400 sq ft	Lab/ Equipment	Lab
ODIN	Madison		Dock/ Warehouse	Shipping and Receiving

In support of the MAF LAN the following on-site space is provided to UNITeS by NASA.

Provider	Location	Amount	Type	Description
NASA	B320	500 Sq Ft	Office	On-site LAN Operations
NASA	B320 Gateway		Shared Equipment	Communications Room
NASA	B102 Node Rm		Shared Equipment	Communications Room
NASA	Various across campus	70 rooms	Shared Equipment	Small Communications rooms for Access Layer devices
UNITeS	Bradford Dr		Office	Engineering, Management, and Business offices – co-located with NISN WAN engineering

In support of the NSSTC LAN the following on-site space is provided to UNITeS by NASA.

Provider	Location	Amount	Type	Description
NASA	NSSTC	1250 sq ft	Office	On-site LAN Operations
NASA	Various across campus	7 rooms	Shared Equipment	Small Communications rooms for Access Layer devices
UNITeS	Bradford Dr		Office	Engineering, Management, and Business offices – co-located with NISN WAN engineering

4.10.8 Network Services

4.10.8.1 IPAM

All three LANs, (MSFC, MAF, and NSSTC) utilize IPAM devices to support DHCP and DNS. Each location has a minimum of two IPAM devices on-site to support these functions.

4.10.8.2 RAS

The MSFC LAN utilizes both dial-up and VPN technologies for remote access. Two Cisco access routers with digital modem cards are used to provide dial-in access. The MSFC LAN has recently installed redundant Cisco ASA5500 series security devices to provided VPN access to the MSFC LAN.

The MAF LAN does utilize a Cisco ASA5500 series security device for VPN access for network management and administrative purposes. All MAF user VPN requirements are satisfied via the MSFC VPN. Only network management VPN accounts are granted on the MAF VPN.

4.10.8.3 NTP

All three of the LANs utilize the Agency provided NTP time sources.

4.10.8.4 Guest Network

All three of the LANs provide a guest network for visitors. The guest networks are logically isolated from other on-site networks. The guest networks are primarily accessed via the wireless LANs, however wired guest is also available in select locations. Guest networks have firewall protected access to the Internet with typical out-bound access and no inbound access. Access into the Private networks is allowed only via VPN connections.

4.10.9 Data Services

4.10.9.1 MSFC LAN High Level Description

The MSFC LAN is a redundant, traditional tiered architecture consisting of a network core, distribution layer, and access layer which connects end nodes to the network. The architecture supports approximately 14,000 switch ports on the MSFC campus, and is scalable. Both the core and the distribution layers are redundant, with Uninterruptible Power Supply (UPS) to maintain services and speed recovery from outages of up to several hours. Access layer switches are not normally supported with UPS. The core can support sustained multi Gigabit transmission, and the access layer connects end nodes to the network at default 10/100/1000 Megabit per second (Mbps) rates in most cases. Upgrades are scheduled for late 2008 and early 2009 to bring all end-system access to the network up to 1Gbps across the center where cable plant supports 1Gbps and backbone circuits within the Core to mesh to 10Gbps.

The MSFC LAN uses Cisco Catalyst 4500 Series switches running native Cisco IOS as the primary access switch. In some areas of low port density, Cisco Catalyst 3550 or 3560 Series switches are used. Upgrades are scheduled for late 2008 and early 2009 that will replace some Cisco 3550-24 switches where multiple switches are located with Juniper EX-3200 and EX-4200 48 port switches. Each access layer switch directly connects into a pair of distribution layer switches or in some cases via a fiber aggregation switch that connects directly to the Distribution nodes. These are typically Cisco 6500 Series switches or Cisco 3750 Series switches running native Cisco IOS. Large buildings contain one pair of network Distribution layer switches. Some small/medium buildings connect to a remote Distribution layer switch. The MSFC core backbone switches are located in 2 separate buildings for redundancy. The cores function as a single core backbone from a networking topology standpoint. Each core location has a pair of backbone routers that are Cisco Catalyst 6500 Series switches running native Cisco IOS software. Each of the four backbone switches connects to two Distribution gateway access switch. The Distribution gateway layer switches also connect to the private firewalls leading to the demilitarized zone (DMZ), as well as the NASA Wide Area Network (WAN). Most core and distribution devices have terminal servers attached to the console ports to allow remote access via an out of band connection.

The MSFC LAN actually consists of three LANs, the MSFC Private LAN, the MSFC Public LAN, and the Guest LAN. The MSFC Private LAN is the main LAN on campus servicing user desktops and most other LAN connectivity needs. It has two server farm locations that house MSFC local server needs. The MSFC Private LAN has wireless connectivity campus wide. The MSFC Public LAN is physically separated from the MSFC Private LAN. The MSFC Public LAN is used primarily for devices such as servers that are accessed from public networks, such as public websites. The access into and out of the MSFC Public LAN is controlled by firewalls. The MSFC Guest LAN is logically isolated from the MSFC Private LAN and is predominantly accessed via wireless connections. Additional logical LANs may be required to support the proposed NASA NCI network architecture.

4.10.9.2 MAF LAN High Level Description

The MAF IT environment is rapidly changing and will likely remain in such a state of flux for the next few years. The primary driver for the changing environment is migration of work from the manufacturing of Shuttle External Tanks (ET) to manufacturing of spacecraft components for the Constellation Program. As a result two LANs currently support the MAF users, the ET LAN supporting ET requirement and the MAF LAN (MLAN) supporting all other NASA requirements on campus. The ET LAN is supported and operated by the ET manufacturing contractor, Lockheed Martin, and will remain so until Shuttle Fly-out currently scheduled for FY2010. Due to the soon approaching decommissioning of the ET LAN it is not part of the NICS contract.

The MLAN will be part of the NICS contract and will be the only NASA support LAN at the MAF upon ET LAN decommissioning. The UNITeS contractor provides network scheduling, network monitoring, network control and system management, problem management, LAN engineering support, LAN operational support, and control centers in support of the MLAN.

A major upgrade to the MLAN is currently underway and this overview will describe the expected state as of March 2009. The MLAN is designed with a traditional multitier architecture with Core, Distribution, and Access tiers. The core is comprised of two Cisco 6500 series switches that are located in two separate buildings to provide geographical diversity. Core devices are connected to distribution layer switches via 10Gbps links. Distribution devices consist of 4 pairs of 6500 series switches. All core and distribution devices are powered via UPS battery systems. The access layer consists of a variety of Cisco switches including the following models: 3560 series, 3750, 2960 series and 6500s. The connectivity between the distribution and access layers varies depending upon the available media type, the user population at the access switch location, and the access layer switch capabilities. When available the preferred uplinks for connectivity are redundant 10Gbps links, however 1Gbps redundant, 1Gbps single attached, and 100Mbps single attached links are also used in some locations.

The manufacturing environments at MAF campus create large geographical footprints with a low LAN user population density. The distance between the access switch and the user often exceeds the 100 meter twisted pair limit and results in multi-mode fiber being used as the media of choice for many users connections.

The MAF LAN supports multiple logically isolated virtual networks including a management network, a private user network (main network), and a guest network. Each virtual network is logically isolated via technologies such as VLANs, Trunks, and VRFs.

4.10.9.3 NSSTC LAN High Level Description

The NSSTC is designed with a multi-tier architecture. The core and distribution tiers are collapsed into the same chassis with a traditional access tier. The core/distribution is comprised of four Cisco 6500 series switches that are located on each floor of the main building. All core devices are powered via UPS battery systems. The access layer consists of a variety of Cisco switches including the following models: 3560, and 2950 series. The connectivity between the core devices is 10Gbps links. Connectivity between core and access layers devices are 1Gbps redundant links. The NSSTC LAN is connected back to the MSFC campus via leased dark fiber (approximately 15 mile circuits). At MSFC a 6500 series switch is used to terminate these links, provide connectivity for Voice over IP traffic back to the MSFC telephone switch and provided connectivity for NASA related user data.

The NSSTC LAN supports multiple logically isolated virtual networks for both the NASA and UAH clients. Each virtual network is logically isolated via technologies such as VLANs, Trunks, and VRFs.

4.10.9.4 Wireless Networks

All three networks provide wireless connectivity. Although operated independently, efforts have been made to make the wireless users environment similar at all three locations. At this time the same wireless profiles can be used at MAF and MSFC. An upgrade at NSSTC should be complete by contract change-over that will bring NSSTC into a similar configuration. A high level description of the three wireless environments is as follows:

a) MSFC Wireless LAN

In addition to the wired MSFC LAN, a wireless LAN is also provided center-wide. The wireless LAN is based on a Cisco Unified design solution, which combines centralized wireless controllers with Lightweight Access Point Protocol (LWAPP) and Control and Provisioning of Wireless Access Points (CAPWAP) enabled access points and wireless management systems.

MSFC offers both a private and a guest wireless 802.11b/g network. Authorized private network user traffic is carried over LWAPP/CAPWAP tunnels. The wireless LAN supports 802.11i security standards for encryption, and 802.1 x frameworks is used for authentication. Guest wireless access requires the acceptance of the Acceptable usage policy and it available to visitors on-site. All guest traffic is tunneled to a guest wireless controller.

b) MAF Wireless LAN

The MAF campus has total 802.11bg wireless coverage. The wireless network uses Cisco based hardware with model 1242 access points, Wireless Service Module (WiSM) controllers, and model 4400 Wireless LAN controllers (WLCs) used as anchor controllers. The wireless access points connect to the access layer of MLAN and utilize LWAPP/CAPWAP tunnels to connect back the wireless controllers. The wireless network does transport some ET production related data and therefore has Service Level Agreements and Operations Level Agreements with the ET contractor. ET related traffic is tunneled to a wireless controller located on the ET LAN.

c) NSSTC Wireless LAN

The NSSTC campus has total 802.11b wireless coverage. The wireless network uses Cisco based hardware with model 1200 access points. The NSSTC wireless LAN may be upgraded to 802.11a/b/g with LWAAP/CAPWAP technology in the near future.

4.10.9.5 Network Security

The UNITeS firewall team maintains, configures, and operates all firewalls on the MSFC LAN, MAF LAN, and NSSTC LAN. Often firewalls are deployed as a redundant pair of devices. Depending on the hardware and the environment the devices may be deployed as an active/standby or as an active/active mode. The following firewalls are maintained:

a) MSFC Public Network Set – Protects the MSFC Private and Guest LANs
b) MSFC Private Network Set – Protects the MSFC Public LAN
c) NSSTC Firewalls – Protects the NSSTC LAN
d) MLAN Firewalls – Protects the MAF LAN
e) Project Level Firewalls – Internal firewalls attached to the MSFC Private LAN
f) Hardware Simulation Lab (HSL)
g) Test Area Network (TAN)
h) Image Analysis Facility (IAF)
i) Education/Training Facility (ETF)
j) Engineering Directorate LAN (EDLAN)

The MSFC Private Network Firewalls screen data destined for the network for the desktop users at MSFC. The Public Network Firewalls screen data both to and from servers whose primary function is to service external users. Juniper (Netscreen), Checkpoint/Nokia and Cisco products are used for these firewalls.

Two Vital Security Web Appliances, model NG-8000, are deployed at MSFC. The NG-8000 is an IBM blade chassis with 14 hot-swappable HS-21 blade servers with the option to expand to 28 servers (14 servers per chassis). Additionally, two Vital Security Web Appliance NG-5100 devices are used on the guess wireless network. Plans include the addition of similar devices to the MAF LAN. These devices are operated and managed by UNITeS.

4.10.9.6 MSFC LAN Network Operations

The MSFC LAN network management center (NMC) is on-site and provides problem analysis/ resolution and service implementation. It is operated Monday through Friday, 6:00AM to 6:00PM, and during special support periods. The staff is on-call 24x7 support with a 2 hour response time. Calls outside of normal working hours may be responded to via remote access or dispatch to on-site, depending on the nature of the call. The ODIN help desk monitors the LAN management system 24x7 for alarms, opens trouble tickets, and contacts the on-call staff as appropriate.

The NMC is responsible for:

a) Responding to user request such as DNS entries, IP address request, and trouble tickets.

b) Alerting on, notification of, tracking, investigating and resolving network outages. Resolution may require involvement of network engineering, data technicians, or third parties; however problem ownership resides with the NMC.
c) Monitoring and reporting on SLAs
d) Operations of all network management systems
e) Implementation of new network services
f) Responding to IT security events
g) Operate and manage infrastructure access accounts such as VPN accounts, Dial-up accounts, and switch/router admin accounts.
h) Verifying all network infrastructure equipment is configurations are consistent with established security templates
i) Keeping network infrastructure equipment configurations are backed-up and maintained properly

The NMC routinely use the following items in their daily work:

a) What's Up
b) What's Up Netflow
c) Cisco Works
d) Wild Packets
e) Wire Shark
f) Solar Winds Tools Set
g) Fluke LAN Meter
h) Cisco Wireless Control System with Location Management
i) AirMagnet Suite
j) E-Telemetry Locate Appliance

4.10.9.7 MAF LAN Operations

The MLAN has operations support staff located at MAF that provides problem analysis/ resolution and service implementation. The staff provides on-site coverage during standard working hours for a minimum of 8 hours per day, Monday through Friday. When not on-site the staff provides call coverage 24X7. After hours troubles are responded to either by remote access or by dispatch of the on-call person. If dispatch is required, employees are required to be on-site at MAF within two hours of notification. Additionally, the Enterprise Network Management Center (ENMC) located at the Marshall Space Flight Center provides 24X7 layer 2 & 3 support to the MLAN and provides initial problem triage and remote resolution during non-standard work hours.

During the course of operating and managing a local area network, outages or potential outages are required in order to perform maintenance for problem resolution, network expansion and network upgrades. All MLAN activities are scheduled via the Activity and Outage Posting and Notification System (AOPNS).

MAF Operations utilizes the following tools and systems:

a) Cisco Works
b) Observer Sniffer
c) MRTG Server
d) Wireless Control System
e) Syslog Server
f) Netflow Collector
g) AirMagnet Suite
h) What's UP (NISC Maintained)
i) 2 DHCP/DNS (IPAM Maintained)
j) E-Telemetry Locate Appliance

4.10.9.8 NSSTC LAN Operations

The NSSTC has operations support staff located onsite that provide problem analysis/ resolution and service implementation. This area is staffed during standard working hours for a minimum of 8 hours per day, Monday through Friday and provides the ability for customers to report outages and troubles. When not on-site the staff provides call coverage 24x7. Troubles occurring outside of normal business hours are responded to by remotes access or dispatch of the on-call person as best effort response.

NSSTC Operations utilizes the following tools and systems:

a) Cisco Works
b) Cisco Secure ACS server
c) MRTG Server
d) DHCP/DNS (IPAM Maintained)

4.10.9.9 Network Processes

Information to be provided by Center, not yet available.

4.10.9.10 Network Lab

The ODIN contractor provides a 400 square foot lab for the LAN. The lab is used for testing network designs prior to deployment, recreating network environments to aide in problem

resolution, burn-in network equipment and other tasks. The lab has sufficient power and environmental controls to allow for multiple large network devices to operate concurrently. The lab equipment is included in the attached equipment listing and could vary depending on the activities being conducted. The lab will typically include at least one of any device present in the network, two if the device is normally installed as a primary/secondary pair.

The MAF and NSSTC LANs do not have a dedicated lab. They do typically stock sufficient hardware in a large communications room to do small scale testing and equipment burn-in. In the event a large scale mock-up, test, or burn-in is needed, then space is requested from other shared network labs or other areas suitable for such a task.

4.10.9.11 Hardware Description

A detailed property listing can be found in the attached equipment listings. However, to estimated property types and quantities are included in this section to aide in how the equipment is utilized in the LAN.

The MSFC LAN utilizes the following equipment:

Description	Usage	Quantity
Cisco 6500 series	Core and Distribution devices	36
Cisco fixed port switches (3550/3560/3750)*	Access layer devices	230
Cisco 4500 series	Access layer devices	120
Cisco small routers (1800/2800/3800)	Access routers providing T1/DSL service to small buildings	30
UPS battery backups	Core and Distribution backup power	24
Cisco ACS servers	Wireless/VPN/Dial-up authentication	4
Cisco ASA device for VPN	Remote Access	3
Cisco 5300 servers	Dial-up Access	2
Cisco NAM blades	Packet Capture/Statistics gathering	32
Cisco 802.11b/g access points	Mostly indoor coverage, LWAAP/CAPWAP, migrating to 802.11a/b/g/n	640
Cisco Wireless Service Modules (WISM) integrated	Wireless LAN	6

with Catalyst 6500 switches		
Wireless control system	Wireless LAN	1
Wireless location appliance server	Wireless LAN	1
Avocent terminal servers	Remote console access	10

* Approximately 40 Cisco Fixed Port switches will be replaced with replaced with Juniper devices in FY09

The MAF LAN utilizes the following equipment:

Description	Usage	Quantity
Cisco 6500 series	Core Devices	2
Cisco 6500 series	Distribution Devices	8
Cisco fixed port switches (3550/3560/3750, 6500)	Access layer devices	75
Cisco 1242	Wireless access points/radios	275
Cisco ACS servers	Wireless authentication	3
Cisco ASA device	Firewalls	2
Cisco Wireless Service Modules (WISM) integrated with Catalyst 6500 switches	Wireless LAN	2
Wireless control system	Wireless LAN	1
IP KVM	Remote access for administrators	2
Cisco 2800 series routers	Remote Console access	3
Cisco IDS blades	Intrusion detection	2

The NSSTC LAN utilizes the following equipment:

Description	Usage	Quantity
Cisco 6500 series	Core Devices	4
Cisco fixed port switches (3560, 2950)	Access layer devices	25

Cisco 1200 series	Wireless devices	15
Cisco IDS blades	Intrusion detection	1

4.10.9.12 Hardware Refresh

The MSFC LAN has a seven year plan document. This document describes the projected refresh needs and associated budget for the next seven years. This document is updated every year to reflect any changes that have occurred. The exact refresh interval may vary based on the equipment and technology; however the goal is to refresh most network equipment every five years. The plan attempts to develop a multiyear budget that minimizes funding variance from year to year and maintains an even funding level requirement.

The MAF LAN is in the process of creating a seven year plan. The LAN just been initiated over the last few years and original equipment life cycles are not yet complete, therefore no refreshment has occurred to date. The goal is to develop the seven year plan with budget data and a refresh frequency of five years.

The NSSTC LAN is refreshed on an as needed basis. As end of life notices are published by the manufacture, equipment is targeted for replacement. Once targeted the replacement cost and schedule is developed.

4.10.10 Collaboration Services

Information to be provided by Center, not yet available.

4.10.11 Customer Relationship Management

Both ODIN and UNITeS have customer relationship personnel that support the LANs as well as other areas of the respective contracts. Often LAN engineers work directly with the customer to define requirements and develop LAN solutions. The following tables contain network demarcation information and "touch points" to other local area networks at the Center.

External/Perimeter/Off-site/Near-Site

None - MSFC LANs at MSFC, NSSTC, and MAF do not interface with any off-site networks.

Internal

MSFC interconnections to other networks at MSFC

Interface Name	Supporting Organization	Description
Huntsville Operations Support Center	Colsa	The MSFC LAN interfaces to the HOSC LAN (also located on the MSFC campus) via a direct fiber cable. The

(HOSC)		connections are made outside the MSFC Firewall.
NASA Data Center (NDC)	SAIC/UNITeS	The NDC is located on the MSFC campus. The MSFC LAN has access to the data center via NISN only.

MSFC Interconnections to other Networks at MAF

Interface Name	Supporting Organization	Description
External Tank LAN	Lockheed Martin	The MAF LAN interfaces to the External Tank LAN (also located on the MAF Campus) via the MAF NISN router. The MAF LAN wireless LAN also transports layer 1 & 2 ET LAN traffic (logically isolated from MAF LAN).

MSFC Interconnections to other Networks at NSSTC

Interface Name	Supporting Organization	Description
University of Alabama – Huntsville (UAH)	UAH	The NSSTC LAN interfaces to the UAH LAN. The NSSTC LAN transports layer 2 UAH traffic (logically isolated from NSSTC LAN)

4.10.12 IT Security

4.10.12.1 MSFC IT Security

The ODIN contract performs the task necessary to develop and maintain the security plan for the LAN equipment. The contractor has developed a standard configuration template based on Center for Internet Security (CIS) guidelines and documented any variances. This template is applied to all applicable devices. Working with UNITeS, ODIN performs network vulnerability scans at a regular interval, evaluates the results, indentifies any discrepancies and remediates at needed. The ODIN Network Management Center response's to incidents 24x7 as notified by the Marshall Incident Response Team (MIRT).

4.10.12.2 NSSTC and MAF IT Security

UNITeS IT Security manages the MLAN and NSSTC LAN security plans and coordinates between other organizations as appropriate. Intrusion Detection services are provided via staff at MSFC on an 8x5xNBD basis. Incidents are responded to according to the Marshall Incident Response Team (MIRT) policies and procedures.

4.10.13 Cable Plant Services (RESERVED)

4.10.14 Emergency Warning Systems (RESERVED)

4.10.15 Public Address Systems (RESERVED)

4.10.16 Radio Services (RESERVED)

4.10.17 Telephone Services (RESERVED)

4.10.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.10.19 Cable Television Services (RESERVED)

4.10.20 Continuation of Center Zoned Architecture Project (CZAP)

The MSFC NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.10.21 Ongoing Center-Specific Projects

The MSFC LAN is currently working to replace network equipment as part of the network technology refreshment activities. These replacements are targeting replacement of existing assets with similar items. No changes are currently expected to the overall LAN architecture.

The MAF LAN has just finished a significant wireless deployment. Over the next few years the MAF LAN is expected to grow to support more users and manufacturing needs, however the exact needs and requirements have not been defined to date. Generally these expansions will require additional access layer and wireless devices to be deployed as the requirements materialize. The overall LAN architecture was developed with expectation of growth and can accommodate significant growth at the access layers before large architectural changes are required.

The NSSTC LAN is currently replacing some wireless devices and near end of life equipment. These refreshments should be complete prior to current contract end and will not result in a significant architectural change or network growth.

4.10.22 Work Load Indicators

Below are some of the work load indicators for these LANs. All quantities are per month unless noted otherwise.

Work description	MSFC	MAF	NSSTC
IPAM data updates	130	8	25

New or updated remote access accounts	80	<1	<1
Number of guest accounts	NA	NA	NA
Network trouble tickets	100	2	180
Network moves, adds, changes	220	2	
Network service requests	4	2	2
IT security incident response support	25	<1	3
Firewall rule changes	28	10	12
Security documentation packages	<1	<1	<1
Telephone trouble tickets	NA	NA	NA
Telephone moves, adds, changes	NA	NA	NA
Telephone service requests	NA	NA	NA
Network projects greater than $500K	3/yr	1/yr	<1/yr

4.10.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.11 NASA SHARED SERVICES CENTER (NSSC)

The NASA Shared Services Center (NSSC) opened March 1, 2006, on the grounds of Stennis Space Center in Mississippi, and is a public/private partnership between NASA and Computer Sciences Corporation. The NSSC consolidated selected activities from all NASA Centers in the areas of Financial Management, Human Resources, Information Technology, and Procurement.

Currently the NSSC is located primarily within Building 1111, with approximately 10 users located in Building 1100. ODIN System Administration support personnel are located in Building 1201. The NSSC is supported by a single network, and there are approximately 500 network users. Building 1111 was constructed in 2008, therefore the infrastructure is new and there are no environmental issues such as asbestos.

4.11.1 Property/Inventory

The ODIN contractor tags and tracks network assets in accordance with the ODIN contract. Government owned equipment is tagged and managed by NASA property custodians

4.11.2 Shipping/Receiving/Inspection

The ODIN contractor provides for shipping, receiving and inspection services for all hardware/software procurements in support of the contract.

4.11.3 Vehicles Necessary to Support Center Work

NSSC users and equipment are all located within close proximity. No dedicated vehicle is required for NSSC support.

4.11.4 Physical Security

All communications facilities and closets have access limited by badge, cipher-lock or key-lock.

4.11.5 Emergency Management

In the case of an event where NSSC is unable to conduct business at its current facilities, contingencies are to initially relocate to a prearranged SunGard facility. If the anticipated downtime duration is long term, NSSC will activate the MSFC Cold Site, which is located in the Intergraph building complex.

4.11.6 Safety

Site specific health and safety plans are required in the execution of work on the communications infrastructure to help identify and control potential hazards such as: electric shock, confined spaces, fall hazards, and noise. Deviations from these plans can result in an order to stop work.

Special training and personal protective equipment are routinely required and could include the use of safety glasses, hard hats, boots, gloves, and hearing protection. The NSSC adheres to all health, safety, and environmental rules and regulations. In addition, OSHA has the right to visit and inspect construction activities.

4.11.7 Facilities

ODIN Network personnel occupy onsite space in SSC's Communications Building, Bldg 1201. This ODIN team supports both NSSC and SSC from this facility. Since this facility is owned by SSC, a description of the facilities, as well as occupancy arrangements can be found under this paragraph of the SSC section below.

4.11.8 Network Services

Basic Network Services are Domain Name Service (DNS) resolution, Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP) and Guest Network Service.

4.11.8.1 IPAM

DNS resolves IP hostnames to IP addresses and is provided by centrally managed Agency DNS servers. Local Network Operations staff provides periodic updates to the DNS database. DHCP allows network devices to be automatically configured using a central database and is provided by centrally managed Agency DHCP servers.

4.11.8.2 RAS

There are two ASA5510 being used as VPNs. Each is licensed for 100 simultaneous connections. The ASAs are configured to work with the Cisco VPN client, NAC, and RSA tokens.

4.11.8.3 NTP

NTP provides a mechanism where all system clocks may be synchronized and is provided from NSSC timing servers.

4.11.8.4 Guest Network

The NSSC guest network is attached to the primary border router and running an OSPF into the firewall. It has both wired and wireless connections. There are 6 user switches (3750) one of which is used for the router, and one of which has the integrated wireless controller.

4.11.9 Data Services

4.11.9.1 High Level LAN Description

The NSSC operates on a single network. The backbone of the network is consists of a distribution, core, and access layer switches. The two border switches and two core switches act as both distribution and core layer switch. The border switches connect to NISN via Border Gateway Protocol (BGP). The border switches contain the centers firewall. The firewall blade in the primary border switch in configured to be redundant with the secondary. The two core switches are also redundant. The core switches have Intrusion detection modules (IDSM) blades in them monitoring all Virtual Local Area Networks (VLANS). There are two voice gateways connect to the core switches and Stennis Space Center's (SSC) telephone switch via four Primary Rate Interfaces (PRIs). One PRI is dedicated to the NSSC's Contact Center. There is a NASA DMZ and Public DMZ switch connected to border switches. All eight of these devices are using Open Shortest Path First (OSPF) for connecting between each other. The access layer switches are connect to the core switches and are using Rapid Spanning Tree (RSTP) to prevent layer two routing loops. All servers, phones and desktops are connected to the network with a GigE connection. The NSSC network infrastructure is comprised of the following:

a) Distribution Layer Switches:
    1. 1111-Border-A
    2. 1111-Border-B

b) Core Layer Switches:
    1. 1111-Core-A
    2. 1111-Core-B
    3. 1111-NASA-DMZ
    4. 1111-PUBLIC-DMZ
    5. 1111-Gateway-A
    6. 1111-Gateway-B
    7. 1111-Border-A
    8. 1111-Border-B

4.11.9.2 Wireless Networks

The NSSC wireless network consists solely of the guest network, and is described above.

4.11.9.3 Network Operations

The following network management and monitoring tools are used at NSSC:

a) Monitoring Tools
    1. Cisco Network Operations Manager (voice)

2. Cisco LAN Manager 3.0

b) Management Tools
   1. Cisco Network Operations Manager (voice)
   2. Cisco LAN Manager 3.0

4.11.9.4 Network Processes

Major configuration and change management for the network infrastructure is governed by the NSSC Configuration Control board. Moves, adds, and changes to the network infrastructure are reflected within the network management tools described above.

4.11.9.5 Network Lab

The network lab is managed and operated by the ODIN contractor.

4.11.9.6 Hardware Description

The NSSC network is comprised of the following components:

Service	Qty	Description
LAN	4	6509 Routers
LAN	15	4507R Switches
LAN	2	37500E Switches
LAN	1	3750 with Integrated WLC
LAN	5	3750 Switches
LAN	33	Cisco 1240 Access points
LAN	2	Cisco 3845 Voice Gateways
LAN	2	Firewall Service Module Service Modules
LAN	2	Intrusion Detection Module
LAN	1	IPS 420
LAN	2	MCS7845 Used for the Communication Manager Cluster 6.1
LAN	2	MCS7845 Used for The IPCC cluster 5.1 build 23
LAN	1	MCS7845 Used for Unity

LAN	1	Dell Server used for Cisco Access Control Server
LAN	1	Dell Server used for LAN Manager 3.0
LAN	1	MCS7845 used for Network Operations Manger
LAN	2	MCS7845 for E911 (not currently used)
LAN	1	Media Manager
LAN	1	Digital Media Encoder
LAN	1	Video Portal
LAN	1	MCS 7845 used for MeetingPlace
LAN	1	Cisco Meeting Place 8106
LAN	1	Cisco MARS-100
LAN	2	ASA5510 used as VPNs
VoIP	2	Cisco 3845 Voice Gateways
VoIP	2	MCS7845 used for the Communication Manager Cluster 6.1
VoIP	2	MCS7845 used for the IPCC cluster 5.1 build 23
VoIP	1	MCS7845 used for Unity
VoIP	1	MCS7845 used for Network Operations Manger
VoIP	Approx 500	IP Phones consisting of a mixture between Cisco models 7971, 7936, 7961, 7965.

4.11.9.7 Hardware Refresh

The network hardware refresh cycle at NSSC is as follows:

a) Servers: Three (3) years
b) Switches: Five (5) years
c) Core Switches: Ten (10) years

4.11.10 Collaboration Services

The NSSC utilizes five (5) monitor ViTS systems located in Building 1111 room 132.

4.11.11 IT Security

Information to be provided by Center, not yet available

4.11.12 Customer Relationship Management (CRM)

The Center ODIN Delivery Order Contracting Officer's Technical Representative, along with ODIN contractor outreach personnel and CSC IT service providers, work with organizational ODIN POC representatives to communicate upcoming changes, gathering of new requirements, and soliciting feedback from the customers

4.11.13 Cable Plant Services

The NSSC uses a combination of single mode fiber, multi-mode fiber, cat 6 wiring, and coax. The configuration is as follows:

a) Building 1111 room 143 to building 1201 - 12 strands multi-mode and 202 strands single-mode
b) Building 1111 room 143 to room 197 - 72 strands single mode (only 4 spare strains)
c) Building 1111 room 143 to room 164 - 48 strands single mode
d) Building 1111 room 143 to room 243 - 48 strands single mode
e) Building 1111 room 143 to room 264 - 48 strands single mode
f) Building 1111 room 143 to room 343 - 48 strands single mode
g) Building 1111 room 143 to room 364 - 48 strands single mode

All copper wiring for the data and phone network is CAT6, there is COAX to support the CCTV system.

Wiring closets are as follows

a) Wiring closets in Building 1111
b) One (1) computer room in Building 1111
c) One (1) wiring closet in Building 1100
d) Two (2) wiring closets in Building 1201

4.11.14 Emergency Warning Systems

NSSC is located on Stennis Space Center and uses the services of the existing SSC Emergency Warning System.

4.11.15 Public Address Systems (RESERVED)

4.11.16 Radio Services (RESERVED)

4.11.17 Telephone Services

The PBX system is a PointSpan M6880 telephony over IP fiber distributed digital telephone system. The system uses proprietary digital telephones manufactured by Aastra Intecom. The voicemail system is also manufactured by Aastra and integrated into the PBX system. The host PBX location is powered by dual UPS systems with a generator backup and a rectifier system with separate battery backup. There are 115 PRI commercial trunks handling the local and 800 calls from SSC. There are also 115 PRI FTS trunks that handle the long distant and international calls. There is 1 PRI incoming only trunk that handles the NSSC Call Center, that feeds into the PointSpan ACD system, which is used as backup should the VOIP IPCC system go down. The PointSpan system is able to provide various telephone features, some of which include CallerID, call forwarding, call pickup etc. The system also has an integrated conferencing system which allows for 3-way, 7 party and 12 party (meet me) conferences. As the NSSC utilizes primarily VOIP there are very few moves, adds or changes dealing with the PointSpan system. The PointSpan system provides backup digital phones for the Call Center and analog service for MFD and conference phones.

4.11.18 Voice over Internet Protocol (VoIP)

NSSC VoIP consists of call processing servers, gateways, voicemail servers, e911, IP phones, and un-interruptible power supplies. There are approximately 500 VoIP phone drops, 60 servers, 40 printers.

All network and VoIP are support through the building's UPS power distribution. The following characterizes the NSSC VoIP:

a) Number of Trunks - T1s to the Stennis PBX, 1 which is dedicated to the NSSC call center.

b) Quality of Service Description - Auto QOS for VOIP

c) NSSC Call Center - Utilizes Cisco IPCC 5.0.

d) Includes a public address system called SA Announce (uses the speaker phones for a public address system). SA Announce is a combined effort between CSC and ODIN. ODIN manages the software, runs the DB as well as the server.

4.11.19 Cable Television Services

The NSSC Cable television distribution infrastructure consists of nine (9) video drops throughout the building terminated in flat screen monitors.

4.11.20 Continuation of Center Zoned Architecture Project (CZAP)

Information to be provided by Center, not yet available

4.11.21 Ongoing Center-Specific Projects

Information to be provided by Center, not yet available

4.11.22 Work Load Indicators

Indicator	Approximate Quantities/month
IPAM data updates	30
Network trouble tickets	3
Network moves, adds, changes	30
Network service requests	10
Firewall rule changes	10
Telephone trouble tickets	20
Telephone moves, adds, changes	30

4.11.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

4.12 STENNIS SPACE CENTER (SSC)

John C. Stennis Space Center (SSC) is home to NASA's premier rocket engine test complex, applied earth science research, and technology transfer programs with facilities in more than 300 buildings and occupying over 138,000 acres in Hancock County, Mississippi. Established in the early 1960's, SSC has evolved to a Multi-Agency Federal City for which NASA is the hosting Agency for the 50 plus Federal, State, Military, Educational, and Commercial companies located on the SSC Campus.

Currently the SSC NASA network exists in 50 major buildings and test facilities with network connections in an additional 100 buildings. SSC NASA Network also provides Internet connectivity and firewall support for three (3) tenants – National Data Buoy Center (NDBC), National Marine Fisheries System (NMFS) and Institute for Technology Development (IFTD) on the SSC NASA LAN. SSC also provides operations and management of the incubator company network called Mississippi Enterprise for Technology (MsET) which exists in three (3) buildings. Network connections for all networks are tracked per organization, division and department so that each connected entity, Program or tenant reimburses NASA for that connection. Overall, SSC has grown to provide a 4500 node network with wired and wireless components, which hosts approximately 300 civil servant and 1,400 contractor professionals all key to achieving NASA's mission in these areas.

4.12.1 Property/Inventory

The contractor provides network operations and maintenance for all components of the SSC network infrastructure which consists of approximately 140 network devices and 3000 end nodes.

4.12.2 Shipping/Receiving/Inspection

All shipping, receiving, and inspection for the SSC LANs are conducted by the FOSC contractor. Equipment is transported to the appropriate point of use as required. All equipment is tracked by asset tags per applicable policies.

4.12.3 Vehicles Necessary To Support Center Work

At SSC, ODIN has leased two (2) mini-vans in performance of the work shared between networks and desktop activities.

4.12.4 Physical Security

SSC complies with the NASA Office of Security for Program Protection (OSPP) policy rules and guidelines that cover all NASA Center's and Center associated facilities. The following link provides additional data on OSPP directives on physical security
http://www.hq.nasa.gov/office/ospp

4.12.5 Emergency Management

The SSC Emergency Operations System provides wireless and voice services in the event of disaster that renders the standard SSC network unusable. The system includes a satellite system, a wireless LAN controller and network infrastructure including VOIP telephone services. The contractor is responsible for supporting Emergency Operations Centers operations and functional tests. The network contractor must interface and support the Emergency Operations Center during all events; including but not limited to; participation of personnel on the Hurricane Ride-out Crew.

4.12.5.1 Center Specific COOP Support

SSC assists with communications support on an as requested basis for the specified locations as identified in the SSC COOP plan, SPLN-1040-0005. The SSC COOP plan is not available for review.

4.12.5.2 Service Continuity of Operations Support

The SSC LAN has been designed to be as resistive to operational impacts as possible to emergency events. However, in the event that critical LAN components are non-operational or unavailable the SSC LAN contractor has critical LAN components spared in nearby Building and agreements are in place with manufactures in the event emergency replacements are required. Most of the IT related hardening projects, such as the cable plant and mobile communications vehicles, will be maintained outside of this contract

4.12.6 Safety

Site specific health and safety plans are required in the execution of work on the communications infrastructure to help identify and control potential hazards such as: lead, asbestos, electric shock, confined spaces, fall hazards, and noise. Deviations from these plans can result in an order to stop work. Permits and work plans are required for events such as the use of lasers, lifting devices and cranes; for confined space and electrical substation entry; and excavations. Special training and personal protective equipment are routinely required and could include the use of safety glasses, hard hats, boots, gloves, and hearing protection. SSC adheres to all health, safety, and environmental rules and regulations. In addition, OSHA has the right to visit and inspect construction activities.

4.12.7 Facilities

ODIN Network personnel occupy onsite space in SSC's Communications Building, Bldg 1201. As a Firm Fixed Price Contractor, the ODIN contract is required to pay NASA SSC for this onsite space. Facility costs charged to the contractor are based on SSC's current rates for office and storage space per square foot. Other portions of the building currently house personnel supporting additional ODIN services such as desktop support, back office support, system

administration, radio, and video. Space including a conference room is also allocated to current ODIN program management. The ATT POP and the NISN gateway are also located in this facility. It is SSC's intent that multiple I^3P contractors will be co-located in Bldg 1201.

The space estimate below reflects office space used by dedicated Network technicians/administrators and dedicated space used in network equipment storage. All network communications closets and floor space in other buildings are not included within this response. The following is a listing by type of space.

Type of Space	Square Footage
Office Space	386
Technical Space	0
Storage	240
Lab	0
Conference Room	0
Miscellaneous	0

4.12.8 Network Services

4.12.8.1 IPAM

SSC currently utilizes the Agency provided IP Address Management system and DNS/DHCP servers. IP addresses are currently registered in the IPAM system and are entered into the local SSC network configuration database.

4.12.8.2 Remote Access

Remote Access Services for SSC clients include client-based VPNs terminated on a Cisco 3080 VPN concentrators for IPSec based VPNs. In addition, a Juniper Neoteris SSL VPN and a Cisco Remote Access Server for Dial-In is provided.

4.12.8.3 NTP

SSC currently has two center stratum 1 NTP servers and two center stratum 3 NTP servers. The stratum 3 NTP server is used for telecommunications and stratum 1 for network devices.

4.12.8.4 Guest Network Services

SSC provides for Guest Network Services as follows:

a) Wired Guest - The SSC Open zone offer wired guest connectivity if required by end-user.

b) Wireless Guest - Guest wireless services are available within selected NASA conference rooms/facilities. All wireless Guest network services are managed by Cisco Wireless LAN Solution Engine located in the Bldg. 1201 Network Operations Center.

4.12.9 Data Services

4.12.9.1 High Level LAN Description

The SSC NASA network consists of four major zones separated by a state-full firewall or router access control lists:

a) Open zone which houses the Guest hardwired and wireless services,
b) Public zone which houses the tenants, the Demilitarized zone (DMZ) and Campus zone.
c) Extranet which consists of the Remote Access Server (RAS) for dial-in support and Virtual Private Network Servers (VPN) for remote Internet support
d) Private zone which consists of many Virtual LANs (VLANs) for internal servers, workstations and other network attached devices.

The MsET network consists of an ISP connection which is funded by Center of Higher Learning to the MsET (NASA contractor managed) firewall which is funded by MsET consortium which is a joint effort with the Mississippi Development authority, NASA, and Mississippi Universities, to the distribution switch out to the four access layer switches.

SSC LAN has four network zones as follows:

a) SSC Open Zone

The SSC Open Zone provides system connectivity for the wired and wireless Guest network, and the for SSC's Virtual Private Network (VPN) appliances as well as providing the first layer of defense for the SSC NASA network. Minimal protection is provided via router access control lists. The Guest network is currently limited to NASA conference rooms in NASA occupied space. Guest connections are both hardwired and wireless. IP addresses are supplied both static and via DHCP. The DHCP service used provides quarantining of connections until the end-user agrees to an End-User agreement. The Open Zone provides connectivity to the MsET NASA managed infrastructure via the SSC Checkpoint Firewalls.

b) SSC Public Zone

The SSC Public Zone provides system connectivity to the Demilitarized zone (DMZ) and Campus zone, as well as the SSC Tenants (NMFS, NDBC, IFTD) that utilize the NASA SSC Network connection as a transport to the Internet. The NDBC and IFTD both utilize the

NASA Domain Name Service (DNS). Currently the DMZ and Campus zones are VLANs within the Private area network switches. The DMZ currently allows anyone anywhere to connect to systems via specified services. The Campus zone allows specific networks (selected Tenants within the NASA SSC Fee Area) to connect to systems via specified services. Approximately 200 systems exist between the DMZ and Campus Zones. Tenant connectivity is proxied behind Tenant managed network hardware, so the number of systems associated with each Tenant connected network is not known. The SSC Private Zone provides system connectivity for all remaining systems including NASA Civil Servants and Contractors via the intra-campus system that supports approximately 3500 nodes.

c) SSC Private Zone

The SSC Private Zone consists of Ethernet topology consisting of two Core Layer Switches, three Distribution/Access Layer Switches, and approximately 80 access layer switches and Asynchronous Transfer Mode (ATM) topology. The ATM topology consists of three Core Layer Switches, two LAN Emulation Service/Broadcast Unknown Service appliances, and approximately 15 access layer switches. The ATM topology leverages Layer 2 Emulated LANs (ELANs) and provides end user Ethernet connectivity at 10 Mbps and ATM backbone connectivity at either 155 Mbps or 622 Mbps. The ATM topology is scheduled to be replaced, pending funding, by December 2012. SSC relies heavily within the Ethernet topology on the VLAN architecture leveraging Layer 2 connectivity with backbone connectivity ranging from 100 Mbps, 1 Gbps, or 10 Gbps. End user connectivity ranges from 10 Mbps to 1 Gbps. Over 32 VLANs are in service to segregate broadcast domains and to implement additional network restrictions via router ACLs. All Ethernet and ATM connected end-nodes are tracked in the Network configuration database for network jack to network port relationship, end-node attributes, and point of contact information, Media Access Control (MAC) address, speed, assigned VLAN/ELAN, Internet Protocol (IP) information, and other pertinent attributes. Network end-nodes are secured to Network switch ports by “locking” via vendor supplied software to the end-nodes MAC address. See Security section for further details.

d) SSC Extranet Zone

The SSC Extranet provides a VLAN separation for remote access termination points such as the VPN appliances, the Remote Access Dial-In server, and DMZ/Campus servers with dual Network Interfaces (NICs). The Extranet zone is routed through the Center firewall in order to provide segregation from the Private zone.

4.12.9.2 Wireless Networks

The SSC Wireless infrastructure is implemented on the SSC Open Zone and supports wireless client connectivity and the wireless management network. The SSC wireless network infrastructure consists of a secure Wireless LAN and a guest Wireless LAN.

The SSC wireless infrastructure consists of:

a) Centrally managed Cisco Wireless Access Points that provide wireless services to end users
b) Cisco Wireless Management and monitoring systems

4.12.9.3 Network Security

The SSC Network utilizes "port locking" to secure end-node stations to the designated port on a network switch in all zones. A few exemptions are allowed; specifically, conference room jacks, and test jacks. Test jacks require written justification and conference room jacks are managed. Together they consist of less than 15% of all network connections. Management consists of logically connecting the wiring to the network port but disabling the functionality of the network port. The authorized point of contact must call to authorize the enabling of the network connection for no longer than the day specified. Test jacks require written justification that must be approved by the SSC IT Security manager or SSC Network Manager prior to allowing the network connects to be enabled with no known end-node assigned.

The SSC Network is further segmented by utilizing ODIN managed internal firewalls and ACLs. The two SSC firewalls are centrally managed and monitored by ODIN operations which separate the Open, Private, Public and Extranet zones. Additional separation within each zone is achieved by leveraging ACLs on the SSC network routers. The MsET Firewall (Cisco PIX) provides access control services for the MsET network. The network infrastructure for the MsET is considered part of the SSC Open Network, but will be no longer be part of the SSC Open Network after the NASA NCI project but will require out of band management of the MsET network.

Additionally, the 8e6it appliance, a web security device, is active within the SSC private network. The 8e6it appliance provides URL filtering and blocking to all SSC clients located within the SSC private zone.

4.12.9.4 Network Operations

Network management services are hardware and software applications that provide monitoring and management services for the network infrastructure. This is currently funded from both the ODIN contract and directly from NASA. Currently the hardware implemented includes:

a) Dell Hardware
b) Solaris Hardware
c) Network Monitoring/Management software implemented includes:
d) Network Health – network performance/trend analysis tool
e) Cisco Works – network Cisco monitoring
f) SolarWinds – network polling and system alert generation

g) ForeView – ATM network monitoring
h) Cisco WSLE - wireless system monitoring

An instance of each management package is used to monitor/manage all network zones. IT management displays are available via web browser and are also displayed in the Stennis IT Monitoring Center as well as the Stennis Network Operations Center. The majority of hardware and application software is located in Bldg. 1110 at the Stennis IT Monitoring Center.

The SSC LAN network operations center (NOC) is on-site in Bldg. 1201, utilizing applications hosted in the Stennis IT monitoring center, and provides problem analysis/ resolution and service implementation. It is operated Monday through Friday, 6:00AM to 6:00PM, and during special support periods. The staff is on-call 24x7 support with a 4 hour response time. Calls outside of normal working hours may be responded to via remote access or dispatch to on-site, depending on the nature of the call. The ODIN help desk opens trouble tickets, and contacts the on-call staff as appropriate. The NOC supports seating for approximately five personnel.

The NOC is responsible for:

a) Responding to user request such as DNS entries, IP address request, and trouble tickets.
b) Alerting on, notification of, tracking, investigating and resolving network outages. Resolution may require involvement of network engineering, data technicians, or third parties; however problem ownership resides with the NOC.
c) Monitoring and reporting on SLAs
d) Operations of all network management systems
e) Implementation of new network services
f) Responding to IT security events
g) Operate and manage infrastructure access accounts such as VPN accounts, Dial-up accounts, and switch/router admin accounts.
h) Verifying all network infrastructure equipment is configurations are consistent with established security templates
i) Keeping network infrastructure equipment configurations are backed-up and maintained properly

The Stennis IT Monitoring Center is located in Bldg. 1110 and will not be part of the NICS contract. The Stennis Network Operations Center is located in Building 1201 and provides displays for network management/monitoring hardware.

4.12.9.5 Network Processes

Configuration and change management for all network infrastructures is governed by the SSC Network Board, which consists of SSC Network Manager and SSC IT Security Manager. This board is governed by the SSC CIO and manages the configuration for all SSC IT infrastructures.

4.12.9.6 Network Lab

SSC maintains an on-demand lab within Bldg. 1201 when a mock up of installations are required.

4.12.9.7 Hardware Description

The contractor provides network operations and maintenance for all components of the SSC network infrastructure. The following hardware platforms are utilized to create the SSC network and security architecture.

Quantity	Make & Model	Function
4	FORE ASX1000/200BX	ATM backbone
15	ES3810	Access Layer switches
2	FORE NSX 9500	ATM LECS switch
26	Cisco 6500	Router/Core/Distribution/Access layer switches
20	Cisco 4500	Distribution/Access Layer switches
15	Cisco 3500	Access Layer switches
16	Cisco 3700	Access Layer switches
30	Cisco 2900	Access Layer switches
16	Cisco 1200	Wireless Access Points
2	Resiliance Appliance	Checkpoint firewall
2	Cisco PIX	MsET firewalls
2	Juniper SSL appliance	SSL appliance

Quantity	Make & Model	Function
2	Network Associate GIG	Network sniffer
1	Network Associate DSS 100	Network sniffer
1	Cisco WSLE	Wireless security device
2	Toplayer	Network connection aggregator
1	Symmetricon NTS-200	Network Stratum 1 GPS time server
1	Cisco 5300	Dial-in remote access server
2	Cisco 3080	VPN appliance

4.12.9.8 Hardware Refresh

Information to be provided by Center, not yet available

4.12.10 Collaboration Services

The Current SSC networking contractor does not provide any collaboration services. These services are currently provided by the UNITeS contractor as part of the Wide Area Network services.

4.12.11 Customer Relationship Management

The following tables contain network demarcation information and "touch points" to other local area networks at the Center.

External/Perimeter/Off-site/Near-Site

Interface Name	Supporting Organization	Description
NDBC Network	National Data Buoy Center, 228-688-2505	Resident Agency network attached to SSC NASA network
ITD Network	Institute for Technology Development, 228-688-2509	Tenant network attached to SSC NASA network
NMFS Network	National Marine Fisheries	Resident Agency network attached to

	Systems, 228-688-3103	SSC NASA network
MsET Network	Mississippi Enterprise For Technology, 228-688-3144	Tenant network that managed by Network Contractor but not NASA WAN network, will coordinate with ISP for connectivity

4.12.12 IT Security

The ODIN contract performs the task necessary to develop and maintain the security plan for the LAN equipment. The contractor has developed a standard configuration template based on Center for Internet Security (CIS) and National Security Agency (NSA) guidelines and documented any variances. This template is applied to all applicable devices. Working with ITS contractor, ODIN performs network vulnerability scans at a regular interval, evaluates the results, indentifies any discrepancies and remediates as needed. The ODIN Network Operations Center responds to incidents 24x7 as notified by the SSC Incident Response Team.

4.12.13 Cable Plant Services (RESERVED)

4.12.14 Emergency Warning Systems (RESERVED)

4.12.15 Public Address Systems (RESERVED)

4.12.16 Radio Services (RESERVED)

4.12.17 Telephone Services (RESERVED)

4.12.18 Voice over Internet Protocol (VoIP) (RESERVED)

4.12.19 Cable Television Services (RESERVED)

4.12.20 Continuation of Center Zoned Architecture Project (CZAP)

The SSC NCI CZAP will focus on making future necessary modifications to comply with the NASA's network zone architecture, NCI.

4.12.21 Ongoing Center-Specific Projects

SSC is still in recovery mode from Hurricane Katrina which occurred in August 2005. As such, many infrastructure designs, construction, and modifications are on-going and are not scheduled to be complete prior to the transition to the NICS contract. The contractor will be required to assume responsibility for design, installation, and activation of all on-going network expansions and modifications.

4.12.22 Work Load Indicators

Trouble tickets are currently managed by the ODIN Consolidated helpdesk in Madison, Alabama. Tickets are bundled in the ODIN desktop seat. Trouble tickets are currently managed by the ODIN local helpdesk. The monthly average for tickets for networks related activities is approximately 15 tickets per month.

Recent Statistics for Network Trouble Tickets:

a) Additions, Moves, and Changes (total for 2008) – 670
b) Network Trouble Tickets (avg. / month) – 15
c) Network Trouble Tickets (total for 2008) – 180

4.12.23 Applicable Documents

Refer to NICS RFP Attachment J -10, *Applicable Regulations and Procedures* for more information regarding the Center policies and procedures.

5 INFRASTRUCTURE PROJECTS

5.1 UNITES NISN NETWORK COMMUNICATIONS INTIATIVE (NCI) PROJECT

The NCI Project was initiated in FY08 by the OCIO/I^3P, to standardize each Center network border infrastructure across NASA, as a first step to end-to-end network management. The NCI was established to standardize the Center network border infrastructure which consists of a border router, border firewall, proxy server, and supporting network equipment to interface with both the NISN WAN and the NASA Centers' LANs. This infrastructure build-out began prior to the initiation of the NICS contract. The NICS contractor will complete the remaining NCI Project activities.

The NCI infrastructure establishes a zoned architecture to be extended into the Center local area networks. All inter-zone communications must transition through this architecture; No inter-zone routing decision will be allowed outside of this infrastructure. The contractor will be responsible for executing approved firewall rule-set changes to allow communications between zones, as well as designing and executing network configurations to enable service delivery.

NASA Centers', Facilities', and Headquarters' local network environment are in varying stages of readiness to integrate into this infrastructure. The NCI project is responsible for the build out of the NISN WAN. It should be noted that NISN intends to re-use decommissioned equipment where possible. This equipment will be shipped to Marshall Space Flight Center for re-purposing by NISN. The Center-specific descriptions for the Center LAN transition is included in the separate Center Zoned Architecture Project (CZAP) see section 4.0 CZAP Center activities.

For NCI the contractor will be expected to provide all labor, subcontracts, materials, travel, and other direct costs necessary to complete the migration of any remaining local area networks from existing connections to non-NCI infrastructures (including NISN SIP and PIP) to the NCI Center border network infrastructure at each Center.

For more information regarding the NCI project, please refer to the applicable documents, *System Design Document, Network Communications Initiatives (NCI) Network Architecture Approach, Redacted - Network Communications Initiatives (NCI), Agency IT Program Management Board, Key Decision Point (KDP-D) Briefing,* and *Redacted - Network Communications Initiative (NCI), Project Plan, NCI-005*.

RFP Attachment J-1 *Performance Work Statement*, *Appendix D-1* defines the specific baseline scope of work required for the bidding of the continuation of this project.

5.2 CENTER ZONED ARCHITECTURE PROJECT (CZAP)

The Center Zone Architecture Project (CZAP) performs the Center activities necessary to migrate the Center specific equipment to the NCI deployed zones. CZAP is charged with the migration planning and execution of the migration from existing Center LANs architectures to the zone architecture environment. At contract award the following centers will have completed CZAP at DFRC, MSFC and NSSC. The contractor shall complete the CZAP deployments, e.g. CZAP Continuation, at:

a. Ames Research Center (ARC)
b. Glenn Research Center (GRC)
c. Goddard Space Flight Center (GSFC)
d. NASA Headquarters (HQ)
e. Jet Propulsion Laboratory (JPL)
f. Johnson Space Center (JSC)
g. John F. Kennedy Space Center (KSC)
h. Langley Research Center (LaRC)
i. MSFC's Michoud Assembly Facility (MAF)
j. Stennis Space Center (SSC)

Each center is in various stages of preparedness for their Center specific activities for CZAP, refer to Section 4.0 for additional information.

RFP Attachment J-1 *Performance Work Statement*, *Appendix D-2* defines the specific baseline scope of work required for the bidding of the continuation of this project.

5.3 FUTURE MULTI-CAST OPEN SHORT PATH FIRST (MOSPF) PROJECT

NASA is currently in the pre-formulation stage of a future project, Multicast Open Shortest Path First (MOSPF) Transition Project. A large portion of the Mission Network segment, Closed IONet, is required to support UDP multicast requirements with very low packet loss and minimal probability of packets arriving out of order. The only multicast routing protocol that would meet these requirements in 1996 was MOSPF. The Nortel Multiprotocol Router Series was selected for this segment of the Mission Critical Network. Nortel announced in January 2007 that they were dropping this series of routers and that the End-of-Support date would be June 1, 2012. The scope of this project is to identify a new Multicast Routing Protocol and replace the Nortel multi-protocol routers before the end of vendor support. The MOSPF Transition Project is an example of a future project that could be added to the NICS contract after contract award.

The project's objective is to migrate from the multi-cast open short path first protocol, utilized by end-of-life Nortel routers. Nortel is projecting the end of life these routers for June 1, 2012. The draft scope of the project is as follows:

a. Purchase enough equipment to extend us tbd months beyond June 2012.
b. Migrate to an alternate Multicast Routing protocol in the MOSPF Multicast Portion of the NISN Closed IONetwork
c. Replace existing Nortel Routers, 3 Comm hubs and Fiber Distributed Data Interface (FDDI) on the closed IONet
   1) Test, select, procure and install (new) leased equipment including cabling, racks, etc
   2) Implement network augmentation, as required, at 17 NASA Centers and associated sites

The following documents describe the draft plans for the MOSPF Project:

a. MOSPF Draft Requirements
b. MOSPF Draft Transition Plan

It is anticipated that this will be an Indefinite Delivery/Indefinite Quantity (IDIQ) Task order in FY10 and is included in the RFP as a scenario with a requirement for a rough order estimate costs to be provided by the offerror's.

5.4 FUTURE OCIO/I^{3}P INFRASTRUCTURE PROJECTS

The NASA OCIO governance board, Information Technology Management Board (ITMB), has approved at a very high level the pre-formulation of the following transformational projects:

a. Consolidation of Corporate VPN for Remote Access Service
b. Agency Corporate Content Filtering

These transformational projects are anticipated to start after NICS contract award. It is anticipated that these will be IDIQ Task Orders in FY10 and are not to be included in the initial contract value.

5.5 APPLICABLE DOCUMENTS

Located at NICS, Other Documents, B&H Applicable Documents
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. MOSPF Draft Requirements, (MOSPF Requirements.doc)
b. *MOSPF Draft Transition Plan,* (MOSPF Transition Presentation v3 02 02 09 scd.ppt)

The following documents are available on CD-ROM and may be requested in writing on company letterhead from:

Jeff Jackson
OFC: PS31, Procurement Office
NASA, George C. Marshall Space Flight Center
MSFC, AL 35812
256-544-8935
jeffery.s.jackson@nasa.gov

a. *System Design Document, Network Communications Initiatives (NCI) Network Architecture Approach*, (NCI Intranet-023 BASELINE2 (Systems Design Document).doc)
b. *Redacted - Network Communications Initiatives (NCI), Agency IT Program Management Board, Key Decision Point (KDP-D) Briefing*, (OCIO_IT_PMB_KDP_D_NCI_032609.ppt)
c. *Redacted - Network Communications Initiative (NCI), Project Plan, NCI-005,* (NCI-005_(Project_Plan)_BASELINE_1c.doc)

6 UNIQUE SERVICES

6.1 UNITES RUSSIA IT SERVICES

Russia services include all IT support to the NASA facilities that are shared with the Russian Space Agency and are located in Russia and related Central Asia republics. The uniqueness of this service is related to the locations external to the United States and the international cooperation with Russia. This service is specifically funded mission programs that are in collaboration with Russia. The following summarizes the Russia IT Services:

a. Wide Area Network (WAN)
   1) Dedicated (Mission) Voice
   2) Switched Voice
   3) Routed (Mission) Data
   4) Routed (Admin) Data
   5) Video Teleconferencing (VTC)
   6) Facsimile
b. Local Area Network (LAN)
   1) Electronic Mail/SMTP Gateway
   2) Anti Virus Protection
   3) Manual Procedure Viewer (MPV)
   4) Internet Access/SMTP Gateway
   5) Domain Name Services (DNS)
   6) Data Transport (Telnet/FTP)
c. End User Support
   1) PC/Workstations
   2) Laptops

3) Printers
4) Telephones
5) Conference Room

d. IT Security
1) Firewalls
2) Network Metrics
3) Web Trending
4) Incident Response

Additionally they provide the following for the Mission Support for the Houston Support Room (HSR) located at the Mission Control Center Moscow (MCC-M) complex:

a. 24/7 Network Monitoring and Help Desk Support
b. WAN/LAN and Secure NT Domain/Email/Web Server Administration
c. Export Control
d. One stop procurement, engineering, installation, maintenance, and support for IT and telecommunications hardware/software.

6.1.1 UNITeS Russia IT Services Overview

The Russian IT services covers planning, implementation and sustaining support for NASA program and project requirements in Russia, the Cosmodrone and Baikonur. The infrastructure in Russia consists of basic telecommunications and end user workstation/server services that are capable of delivering video, voice, data and mission operations services. The Russia IT service technical monitor is a member of the MSFC CIO.

The locations receiving Russia IT services in the Russia and United States include the following:

a. Russia Hub/Synterra, Moscow, Russia
b. NASA Moscow Liaison Office at the U.S. Embassy
c. Volga Apartments; NASA in country residence
d. Khrunichev State Research and Production Facility
e. Moscow Mission Control Center, the Russian Space Corporation
f. Energia, Gagarin Cosmonaut Training Center
g. Institute for Biomedical Problems
h. Institute for Space Research and the Russian Space Agency
i. Cosmonaut Hotel
j. Sputnik Hotel
k. Baikonur or Kazak Cosmodrome
l. JSC Buildings 30 and 17
m. MSFC Building 4200

6.1.2 Russia IT WAN and LAN and End User Support

The Russian wide area network infrastructure is divided into four (4) circuits. Two circuits service the ISS Mission specific needs of Johnson Space Center (JSC) and two circuits service the network requirements of Mission Support/NASA Corporate/Administrative (e.g. MSFC) needs of NASA. Additional paths are provided on the NISN PIP backbone between MSFC and JSC, which is not managed by the Russian IT services, but are used to facilitate alternate paths if a communication failure occurs in the direct Mission routes from JSC to Moscow and Mission Support/NASA Corporate/Administrative data through Russia IT Services managed firewalls.

The Russia IT service customer base is as follows:

a. NASA Program/Project Offices
b. International Space Station Program Office, Johnson Space Center
c. Mission Operations Division, Johnson Space Center
d. Astronaut Training Division
e. Life Sciences Office
f. International Partners Office, Johnson Space Center
g. Office of Life and Microgravity Sciences and Applications
h. Mission Operations Lab Payloads, Marshall Space Flight Center
i. Office of External Relations, NASA Headquarters

6.1.2.1 Russia Hub/Synterra; Moscow

The primary location for the UNITeS contractors in Russia is the Russia HUB in Moscow located in the subcontractor Synterra facilities. The Russia Hub location provides for UNITeS offices, equipment staging and storage.

6.1.2.2 NASA Moscow Liaison Office (NMLO) ; United States Embassy

The NASA Moscow Liaison Office (NMLO) was established in 1994 for the purpose of providing effective in-country coordination on all aspects of NASA's increased cooperative activities in aeronautics and space with its Russian counterparts. It is located at the U.S Embassy in Moscow.

NASA's cooperative activities with Russia in all fields, including but not limited to human space flight, are significant. The NMLO is the focal point for NASA’s administrative presence in Russia, and represents the Agency across all Centers and areas of endeavor.

The NMLO office is provided connectivity to the Russian services network via a fiber optic network. The Circuit originates in the NASA administrative Hub at Synterra and is connected via E1 at the Embassy. The fiber optic system enters the Embassy at the South Gate and is connected via fiber modem to an equipment room in the area of the NASA office. Services offered span the complete range of services to include data, voice, low bandwidth video, telephone and fax.

6.1.2.3 Volga Apartments; Moscow

The Volga Apartments is a three star complex consisting of (16 floors, 230 flats) built in 1977 and renovated in 1990. The hotel is located in a quiet and secure area of Moscow, not far from the city center and serves as the residence of NASA and contractor personnel living in Moscow on a permanent or extended stay.

The Volga offers one, two and three room apartments that are furnished for the occupants. Within the Volga Complex, each apartment is provided with data and telephone service, providing the occupants local service to the United States. Available in the Volga is a furnished conference room with audio/video teleconferencing, fax, and printing services.

The Volga Apartments is provided connectivity to the Russia IT services network via a fiber optic tail circuit. The circuit originates in the NASA administrative Hub at ITMS and is connected via 10Mbps to Volga Apartment 61. From Apartment 61, services are routed via Ethernet cabling to the roof then downward to the living quarters.

6.1.2.4 Gagarin Cosmonaut Training Center (GCTC); Star City

The Gagarin Cosmonauts Training Center is located at Star City. Star City is an extensive complex of service and office buildings, where training of Russian and foreign cosmonauts is being carried out. Star City offers facilities for work and leisure for its citizens and guests. It has a secondary school, kindergarten, medical institutions, department stores, various and services. NASA's astronaut corps trains at a location within GCTC called "Territory C", living in cottages and apartments in and around the training facility.

The GCTC office is provided connectivity to the Russian services network via a fiber optic network. The circuit originates in the NASA administrative Hub at Synterra and is connected via 10Mbps to GCTC. Services offered span the complete range of services to include data, voice, low bandwidth video, telephone and fax.

6.1.2.5 Rocket Space Corporation-Energia (RSC-E)

RSC-E is a private Russian corporation. The RSC-E office is provided connectivity to the Russian services network via a fiber optic network. The circuit originates in the NASA communications hub at the Mission Control Center Moscow and is connected via 10Mbps to RSC-E. Services offered span the complete range of services to include data, voice, and low bandwidth video, telephone and fax. RSC-E is also the Russian Services gateway location to the Russian Space Agency launch location at Baikonur.

6.1.2.6 Khrunichev State Research and Production Space Center

The Khrunichev State Research and Production Space Center consist of two of the largest Russian produces of aviation and rocket and space technology; Khrunichev Machine building plant and "Salyut" Design Bureau.

The Khrunichev Space Center provides work for 70 subcontractors. The Khrunichev Space Center provides commercial launch capability (Proton rocket) supplying heavy lift capacity for foreign nations such as the United States.

The Khrunichev office is provided connectivity to the Russian services network via a fiber optic network. The Circuit originates in the NASA administrative Hub at Synterra and is connected via E1 to Khrunichev. Services offered are carrier services, providing multi-service traffic as a connection rather than in support of NASA or contractor personnel. This site, which built the ISS service module, is a member of the ISS team but does not continue to build components for the Space Station effort.

6.1.2.7 Russian Space Agency (RSA)

The RSA has centralized control of Russia's civilian space program, including all manned and unmanned nonmilitary space flights.

The RSA office is provided connectivity to the Russian services network via a fiber optic network. The circuit originates in the NASA administrative Hub at ITMC and is connected via E-1 to RSA. Services offered span the complete range of services to include data, voice, low bandwidth video, telephone and fax.

6.1.2.8 Mission Control Center-Moscow (MCC-M)

The Mission Control Center (MCC-M) Moscow is used to support relevant Space Shuttle missions and the International Space Station. The flight control room (HSG) is where flight controllers get information from computer workstations or from projected displays.

Connectivity to the Russian services network via a fiber optic network, and microwave circuit. The Mission Support/NASA Corporate/Administrative circuit originates in the NASA administrative Hub at Synterra and is connected via E-3 to MCC-M. Services offered span the complete range of services to include data, voice, digital video, telephone and fax. Two additional “Mission” circuits are provided and services consist of data and voice loops. One circuit originates at JSC in Bldg. 30, and the other at the Mission hub at Synterra providing an alternate and diverse path back to JSC via MSFC.

6.1.2.9 Institute of Bio-Medical Problems (IBMP)

The Institute for Biomedical problems performs fundamental and applied scientific-research, experimental-design and technological activities. Activities include training and retraining of researchers, in the field of aviation, space and sea medicine and safety, and, protection of, rescue, and life-support to people under emergency conditions. The institute also collaborates with scientific research institutions in Russia and foreign nations.

The IBMP office is provided connectivity to the Russian services network via a micro-wave network. The circuit originates in the NASA Hub at Synterra and is connected via E1 to IBMP. Services offered include data, voice and fax. No NASA personnel are resident at this location.

6.1.2.10 Baikonur or Kazak Cosmodrome; Kazakhstan

Baikonur Kazakhstan is Russia's largest Cosmodrome. It is the only Russian Space Agency Facility used for manned launches, having facilities for the larger Proton, N1, and Energia launch vehicles.

The spaceport ended up on foreign soil after the break-up of Soviet Union. The official designations NIIP-5 and GIK-5 are used in official Soviet histories. It was also universally referred to as Tyuratam by both Soviet military staff and engineers, and the US intelligence agencies. Since the dissolution of the Soviet Union the Russian Federation has insisted on continued use of the old Soviet 'public' name of Baikonur. In its Kazakh (Kazak) version this is rendered Baikonur.

The Baikonur Cosmodrome extends for 85 km from North to South, and from 125 km from East to West, a territory as great as Moldova. Aside from dozens of launch pads it includes five tracking-control centers, 9 tracking stations, and a 1500 km rocket test range.

There are four (4) locations in Baikonur where NASA has network extensions supporting data and voice. Two locations are located at the launch assembly complex area, Area 254 and Hotel 3, and are controlled by RSC-E, which is the Russia IT gateway path. The remaining two locations are the Cosmonaut Hotel and the Sputnik, which are located in the actual town of Baikonur. The Cosmonaut Hotel is controlled by GCTC. The Sputnik is a private hotel.

6.1.2.11 JSC Buildings 30 and 17

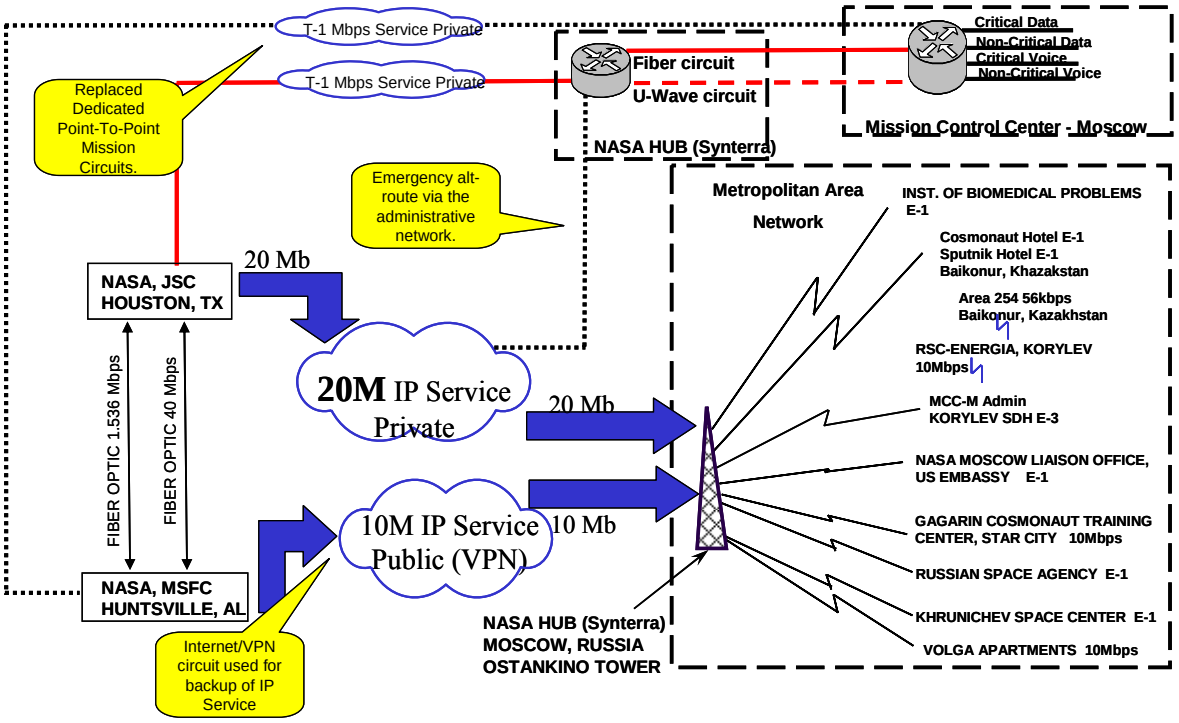
Russia IT Services has network equipment located at Johnson Space Center to support both Mission and Mission Support/NASA Corporate/Administrative services. The JSC gateway is located in Building 17, which is the demarcation of the Mission Support/NASA Corporate/Administrative 20Mbps transatlantic channel, and the PIP path between JSC and MSFC which serves as a logical path for the T-1 Mission alternate route and IP traffic to MSFC. Russia IT services equipment located there is used in support of Video Teleconferencing and PIP data traversing back to MSFC on a dedicated 40Mbps channel. All Mission services are terminated Building 30, including the T-1 transatlantic link directly to the Mission Control Center - Moscow. Russia IT Services equipment located here is used to support real-time Mission data and voice loops to Moscow.

6.1.2.12 MSFC Building 4200

Russia IT Services has network equipment located at MSFC in support of Mission Support/NASA Corporate/Administrative services coming from Moscow via the JSC PIP connection and the alternate route of Real-Time Mission traffic between JSC and Moscow. The MSFC gateway is located in building 4207. Additionally, there is a dedicated VPN channel between the Russia IT Services hub at Synterra and MSFC which serves as a backup route for Mission Support/NASA Corporate/Administrative. Therefore, only one physical circuit

terminates at MSFC which the Russia IT Services manages and that is the alt-route Mission transatlantic T-1. The Russia IT Services staff resides in UNITeS facilities at Bradford.

6.1.2.13 Russia IT Infrastructure



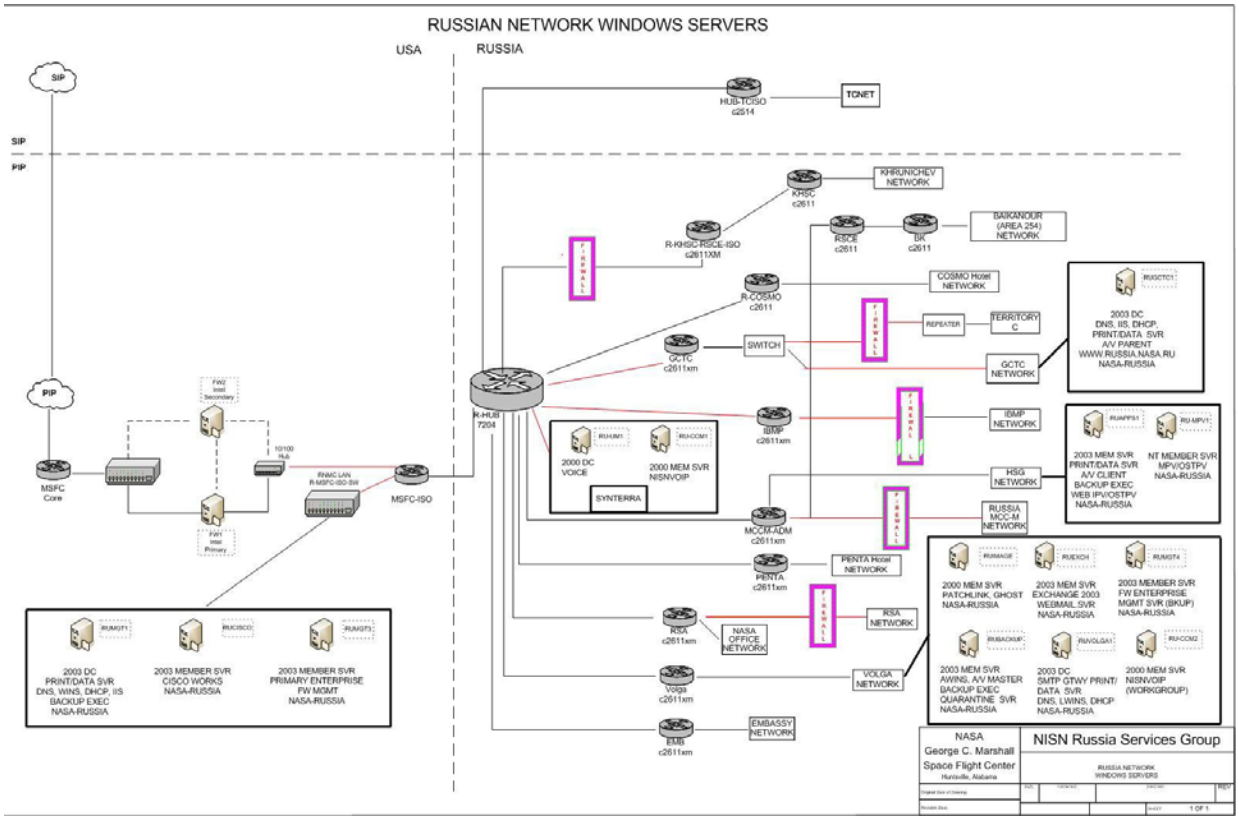
6.1.2.13.1 Russia IT Equipment Distribution

		WAN SERVICES					LAN SERVICES							END USER					ANCILLARY				
	UPS	IDNX Nodes	Channel Banks	Routers	Telephone Switches	Video Teleconf (LBV/ViTS)	LAN Switches	Hubs	NT Servers	SUN Servers	Firewalls	Tape Backup Units	Printers	Desktops	Laptops	Facsimile Machines	Telephones	Satellite Phones	Smart Boards	TVs	VCRs	Projectors	Conference Room A/V
Baikonur	3			1									1		3	1	2						
Embassy	1	1	1	1				3					1	8	2	1	12	1					
GCTC	1	1	1	2	1	3	5		1		1	1	20	48	6	6	78	1		6	4		
IBMP	1	1	1	1		1		1						4		3	10			2	1		
JSC	1	2		3																			
Khrunichev	1	1	4	1		1		5					2	12		1	37			2			
MCCM-Admin	1	1	2	1	1	1	3	1	2		1	2	6	41		6	64		1	1	1	1	1
MCCM-Mission	1	1	2	2		1		4															
MSFC	1	1		2					3		2	1	1										
Penta	1	1	3	1			3						1	3		2	58						
RSA-NASA						1		2					2	5		1	7					1	1
RSA-Russia	1	1	2	1		1	3				1		4	4	3	2	22			2	1		
RSCE	2	1	2	1	0	2				5			13	46	10	4	36			5	2	1	1
NASA HUB	5	2	1	6	1	1					1			1			3						
Volga	1	1	1	1	1	1	2		6			1	13	50		6	56	1		2			1
Other															35								
TOTALS	21	15	20	24	4	13	16	16	12	5	6	5	64	222	59	33	385	3	1	20	9	3	4

Note: All quantities are representative of the equipment located at each site, but do not depict spares or equipment in the process of being excessed or replaced with new equipment.

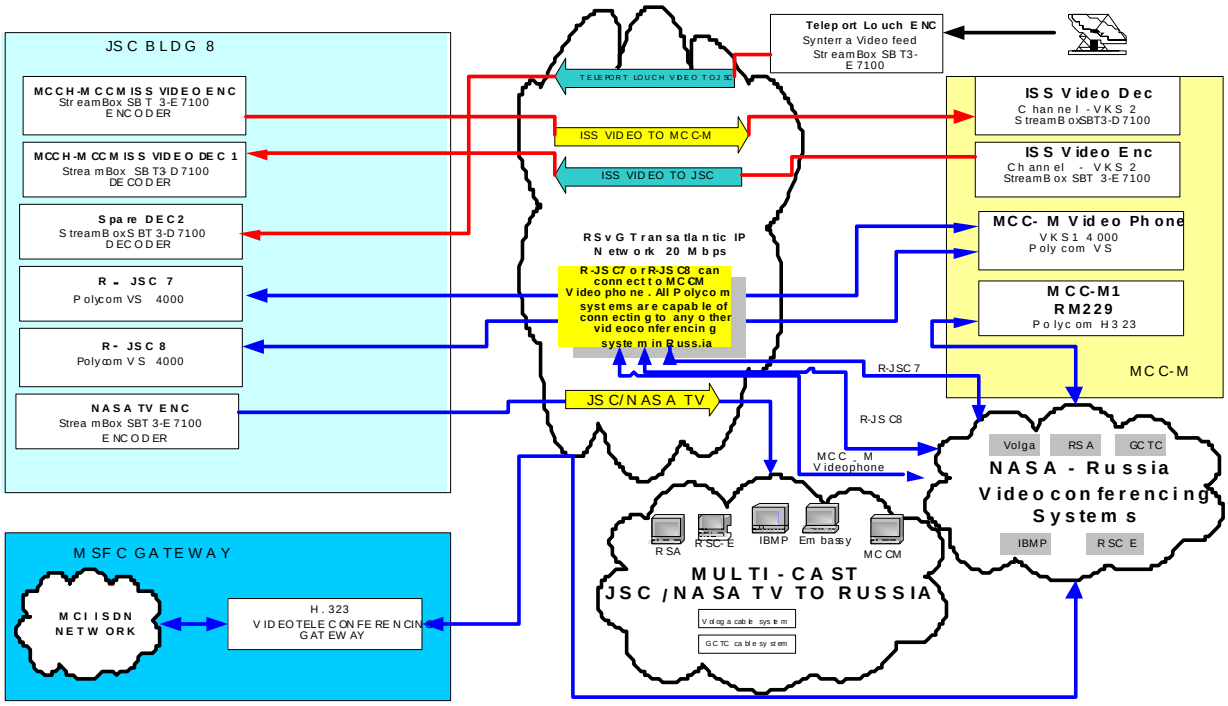
6.1.2.13.2 Russia IT Servers Locations

The following illustrates the servers and service locations on network LANs which support NASA Russia.



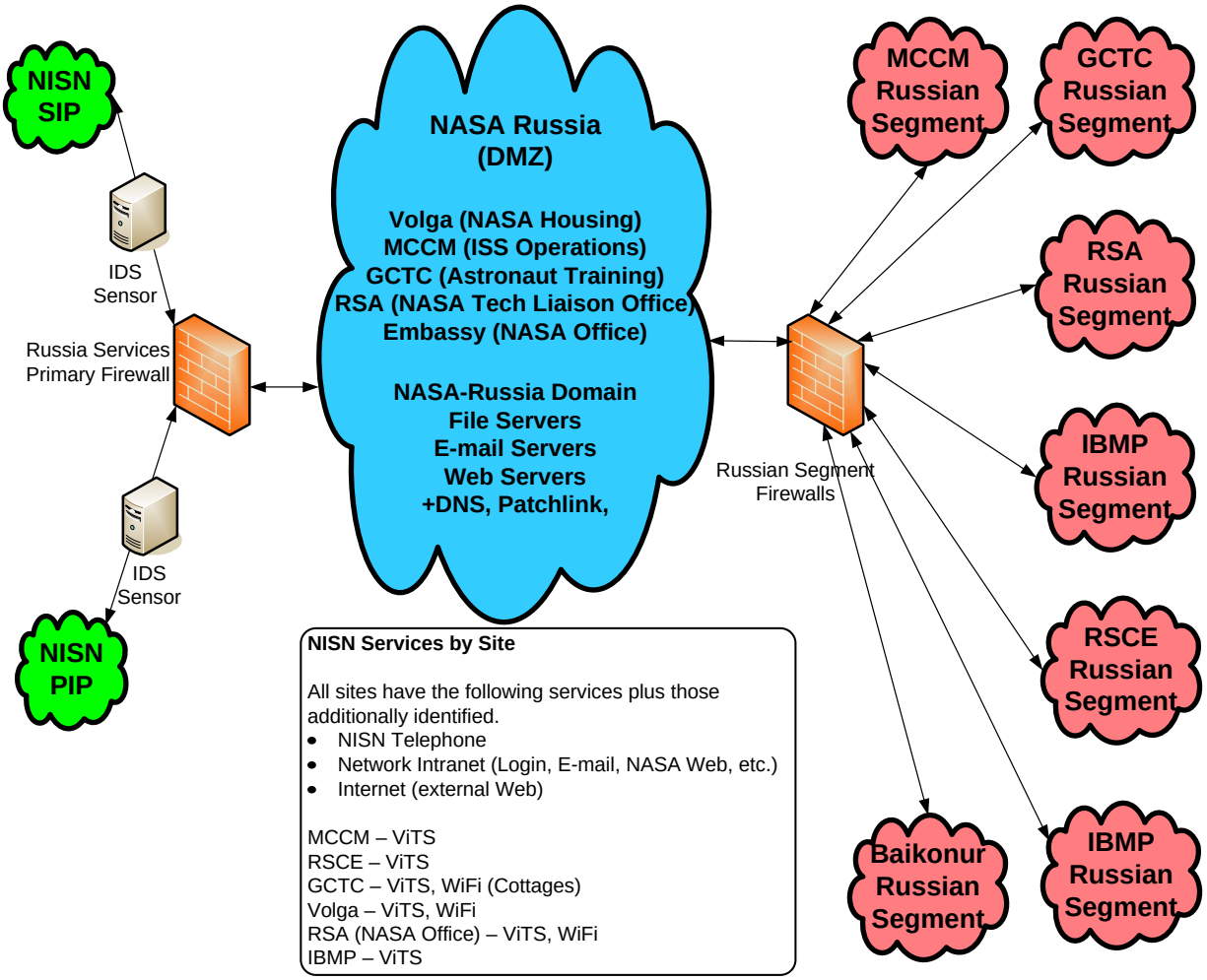
6.1.2.13.3 Russia IT Video Systems

The following illustrates the video infrastructure provided by Russia IT services.



6.1.2.13.4 Russia IT Demilitarized Zone (DMZ)

The following illustrates the Russia Mission Support, Administrative and Corporate network demilitarized zone (DMZ) which support NASA Russia.



6.1.3 UNITeS Russia IT Security

Russia IT Services IT Security procedures apply to all Russian network infrastructures and are defined by Russia IT Services: IT Security procedure 301-001, Russian Services Procedure and Guidelines IS40 Security of Information Technology. The directive is intended for use by civil service and to ensure that safeguards for the protection of the integrity, availability, and confidentiality of users of Russian Services Information Technology (IT). It provides direction for designed IT resources, including data, information, applications, and systems, to ensure those resources can be properly integrated for supporting NASA missions. It is specifically designed to assist those with assigned IT security responsibilities to adequately fulfill those responsibilities.

Several NASA CIO Agency policies play an important role in the overall strategy for the implementation of IT systems. Patchlink updates and reporting are performed just like any other center. Anti-virus systems are used and deployed locally. Intrusion Detection Systems have been deployed at all locations so that not only the WAN can be monitored but also the LANs. This reporting goes directly to the NASA Agency Security teams. Today, there are several initiatives geared to comply with HSPD-12, in which there has been no decision made as to whether they can or will be implemented in Russia, including; 2 factor authentication, Federal Desktop Computing, migration of e-mail to NOMAD. It should be understood that all measures are being taken to integrate the NASA Russia IT architecture to meet the intent of all policies written where possible. The NASA Russia IT architecture was intentionally designed to support Mission Operations in Russia, 24x7. Availability and unique requirements do not fit the standard NASA IT Corporate model, where these systems must support as real-time Mission operations, jointly performed by Foreign Nationals and US Citizens, operating on Russian soil. The Joint Institutional Communications Document and the NASA Roscosmos Intranet Agreement Documents lay-out the framework for these interconnects and operations base. All IT and communications components are purchased, managed and maintained by the Russia IT Services, including computers. These computers are not included in the ODIN contract and have specific "loads-images" to support the unique requirements for real-time Mission operations at the MCC-M and Astronaut training at GCTC.

Where possible, network components are also monitored by the NISN Agency Networks Operations Center, thus utilizing the efficiencies of the contract. Also trouble tickets are logged and maintained through the MSFC NISC Help Desk's Remedy system.

6.1.4 Russia IT Technology Shipping, Export Control and Equipment Inventory

6.1.4.1 Russia IT Unique Export Control

Russia IT services have special procedures, provided at contract award, for Export Control shipments as mandated by NASA HQs and the US Embassy, Moscow (see section 2.5.3). The document, Russia *Services Shipping Instructions*, explains the overall process to ship to Russia.

In FY08, there were approximately ten (10) shipments to Russia by UNITeS. There were also an unspecified number of drop shipments by the contractor's vendors to international locations. The contractor is responsible to insure the proper Export Control procedures were followed and also retains a copy of the necessary documentation of the shipment by the vendor.

6.1.4.2 Russia IT Subcontracting

Contracting and subcontracting in Russia presents some unique challenges that have been overcome by direct negotiations between Government and State agencies in Russia and NASA officials. These challenges have required establishment of unique methods to accommodate Russian business practices and law, yet still comply with US Government contract regulations between the prime contractor and the primary Russian subcontractor. Initially, it must be understood that the Russian government agencies, as well as state-owned organizations and companies, do not recognize a contractor as the legitimate voice of the US Government in making agreements with foreign entities. They do, however, understand the Government and contractor relationships and how payment and contracts are managed. Therefore, when contracts are being negotiated or modified with Russian entities, NASA must be involved with all elements, with the exception of contract value negotiation. This does not exclude the contractor from contacting or working with the Russian officials, State-owned entities, or the vendors themselves. Very few companies in the US have obtained the authority to contract directly with Russian government or Russian owned companies, further compounding the difficulties in making legitimate agreements. Within Russia, all companies must have a 51% minimum Russian ownership, even when partnered with American companies. NASA is also required by law to report to Congress on a bi-annual basis all money which flows to Russia. Reporting procedures, details of which will be provided at contract award..

Currently, Synterra is the prime sub-contractor to SAIC within Russia. Synterra handles all circuit contracts and all subcontracts with the Russian government and Russian companies. Synterra also has a subsidiary, Synterra Media, which provides the incumbent contractor with in-country support. Synterra absolved Telcom Center which was the only Russian company with Government affiliation that had the necessary Russian licenses and approval to provide Russia in-country circuits and on-site services and support for NASA. The Russia IT Services hub, offices, and equipment staging and storage are housed in the Synterra Facility. At every location in Russia where NASA has equipment, there is a subcontract between Synterra and that location (i.e. RSA, Mission Control Center, GCTC, IBMP, etc.) to provide facilities, power, and on-site maintenance assistance. At RSC-Energia, additional IT support is provided for systems/networks that handle ISS Cargo Flow and ISS Inventory systems that interface with NASA database systems in Houston handling the Manifest Data and correlated Cargo Flow systems. Therefore, the current structure of the contract is the prime contractor, who subcontracts to Synterra/Synterra Media, who in turn subcontract to various Russian subcontracts. NASA reimburses the incumbent prime contractor for all allocable and allowable costs. Therefore, SAIC has the contractual authority for purchasing and negotiating costs directly with Synterra and Synterra Media. Synterra and Synterra Media in turn has the authority to contract and negotiate costs for the subcontracts at each of the Russia Government and

Company entities. Synterra and Synterra Media also have the agreements in place that allow their personnel on-site for repairs and assistance to UNITeS.

It is imperative that these relationships and contract agreements be clearly understood as some very difficult lessons have been learned when trying to circumvent the existing contract structure. Several contractors and vendors which have tried to establish other contractual relationships have failed which placed NASA into a position of Mission vulnerability. Currently, the only element of these contract agreements which by nature of competition must be modified or changed is the prime contractor that will be performing NICS services, should other than the incumbent contractor be selected to perform these services. Revised subcontractor relationships within Russia must meet the stringent requirements that currently exist with the existing provider of these services as described within this document. The current contract structure and services are critical to the operations and safety of the ISS and its crewmembers. The current contract arrangements with Synterra, previously Telcom, are the only arrangements which have proven to work since the inception of NASA networks in Russia, in 1994. Offerors proposing a different arrangement must provide documentation sufficient to fully explain their ability to abide by these requirements.

Any alternate method of providing circuits and services in Russia must adhere to the following:

a. An extensive review by NASA and the Russian government must be performed prior to award of the subcontract(s) to determine if the Russian subcontract offer(s) and resulting subcontracts can be recognized as legitimate. This includes compliance with the requirement of the Department of Homeland security for "vetting" the proposed Russian subcontractor, which could take several months to complete.
b. Prepare a proposed migration plan from current subcontracts to new subcontracts whereby all licenses, local agreements, and laws are met.
c. Prepare a proposal for continued operation and location of the NASA Hub in Russia and working locations with no Mission Operations interruptions and outages/restorals in order to meet the NASA NISN baseline requirements.
d. Provide sufficient documentation to ensure that payments to Russian subcontractors are allowed, and have been approved by the Russian government and banking system.

6.1.4.3 Russia Unique VISA

Contractor employees working in Russia are required to use NASA's procedures for obtaining a VISA and are subject to certain restrictions under Russian law including "in-country" work time limits. Applications for these VISAS are available upon request, and are considered to be fully reimbursable costs under the NICS contract. Russian work permits are obtained by NASA in conjunction with Russian Space Agency. Additional information regarding Russian laws and procedures is available through the US State Department website.

6.1.4.4 Russia Unique Procurement

Operations personnel assigned to Russia for long term duty need to have the ability to purchase, in compliance with the Buy American Act, IT equipment and software, on-line via credit card. Such purchases may be shipped to Russia but are often hand-carried by contractor personnel traveling to Russia in connection with contract responsibilities. In-country purchases of such items may also be required depending on circumstances and must be coordinated with NASA personnel in Russia prior to such action.

6.1.4.5 Russia Unique Insurance

Due to differences in standards for medical services provided within Russia and elsewhere, contractor personnel have the option of emergency evacuation or local medical support in Russia using SOS International. SOS insurance is made available by the contractor parent company for purchase. In the event of a medical emergency requiring evacuation to Helsinki or other European facility, SOS insurance must be in place and a guaranteed payment account established in advance. While such insurance and advance payment authorization is not mandatory, unnecessary health risks could occur as a result of delays in evacuation and adequate medical care. Evacuation costs could range from $50,000 to $100,000 or higher and must be paid to SOS prior to evacuation. Further information and cost can be provided directly from SOS International.

6.1.5 Work Load Indicators

The document, *UNITeS NISN Trouble Ticket Summary*, list the type of trouble tickets related to Russia IT Services.

6.1.5.1 Direct Labor Hours

The table, UNITeS Russia Direct Hours FY07 and FY08 depicts the approximate direct labor hours expended in FY07 and FY08 for the services provided by UNITeS for Russia.

		FY07	FY09
UNITeS PWS	PWS Title	Approximate Total Hrs	Approximate Total Hrs
3.5	Russia	30,000	31,000

6.1.6 Operating Procedures

The following documents provide additional information on how the UNITeS Russia IT Services operate:

a) *Check Point & CISCO VPN Client Interoperability Info*
b) *Check Point SecuRemote Installation*

c) *Controlling Nonconforming Product*
d) *Engineering New Requirements: Process Flow and Guide*
e) *How to Create, Update, or Delete a Procedure*
f) *How to Request a Firewall Exception*
g) *IDS Operational Management Guide*
h) *In-Country Loaner-Pool Instruction*
i) *Mission Network Account Management*
j) *NISN Russia Services Emergency Preparedness and Disaster Recovery Plan*
k) *Policies for Computer Setup and Network Access*
l) *Procedures for Creating the Monthly Service Availability Matrix*
m) *Remote Access*
n) *RSvG Change Request Management*
o) *RSvG In-Country Lead Checklist*
p) *RSvG Master Document List*
q) *RSvG Quality Records List*
r) *Russia Mission Routers & Switches Contingency Plan*
s) *Russia Services Group (RSVG) NISC / EMON Circuit Listing and Procedures*
t) *Russia Services Process for Document Approval*
u) *UNITeS Russia Services Group Customer Communication Policy*

6.1.7 Applicable Documents

Located at NICS, Other Documents, B&H Applicable Documents:
http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. *Check Point & CISCO VPN Client Interoperability Info,* (3000-3300-205.doc)
b. *Check Point SecuRemote Installation,* (3000-3300-204.doc)
c. *Controlling Nonconforming Product, (*3000-3300-007.doc)
d. *Engineering New Requirements: Process Flow and Guide,* (3000-3300-101.doc)
e. *How to Create, Update, or Delete a Procedure, (*3000-3300-004.doc)
f. *How to Request a Firewall Exception,* (3000-3300-206.doc)
g. *IDS Operational Management Guide,* (3000-3300-207.doc)
h. *In-Country Loaner-Pool Instruction,* (3000-3300-200.doc)
i. *Mission Network Account Management,* (3000-3300-102.doc)
j. *NISN Russia Services Emergency Preparedness and Disaster Recovery Plan, (*3000-3300-001.doc)
k. *Policies for Computer Setup and Network Access,* (3000-3300-202.doc)
l. *Procedures for Creating the Monthly Service Availability Matrix,* (Service Availability Metric Procedure.doc)
m. *Remote Access,* (3000-3300-203.doc)
n. *RSvG Change Request Management*, (3000-3300-006.doc)
o. *RSvG In-Country Lead Checklist,* (3000-3300-201.doc)
p. *RSvG Master Document List,* (MASTER DOCUMENT LIST.doc)

q. *RSvG Quality Records List*, (Quality Records List.doc)
r. *Russia Mission Routers & Switches Contingency Plan,* (3000-3300-103.doc)
s. *Russia Services Group (RSVG) NISC / EMON Circuit Listing and Procedures,* (RUSSIAN ALARM Procedures ver 1 31.doc)
t. *Russia Services Process for Document Approval*, (3000-3300-003.doc)
u. *Russia Services Shipping Instructions,* (Shipping Instructions.doc)
v. *UNITeS NISN Trouble Ticket Summary*, (UNITeS NISN Trouble Ticket Summary.xls)
w. *UNITeS Russia Services Group Customer Communication Policy,* (Customer Comm Policy.doc)

Located at the Homeland Security Presidential Directives
(**http://www.dhs.gov/xabout/laws/editorial_0607.shtm**)

a. HSPD 12*, Policy for a Common Identification Standard for Federal Employees and Contractors*

6.2 UNITES NATIONAL SECURITY SYSTEMS (NSS) SERVICE IT SUPPORT

The MSFC CIO with UNITeS provides unique agency IT support for HQ's Office of Security Program Protection (OSPP), NSS Service. NSS Service IT Support includes engineering, operations, sustainment and property management of all network and desktop infrastructure for the NSS. The OSPP NSS service provides for a secure communication service between NASA Centers and with other Federal Government organizations. The purpose of NSS is to provide timely distribution of threat information and coordinate disaster response.

UNITeS personnel that provide NSS Service IT Support work typical center hours however they have to provide the following:

a. On Call Service for OSPP designated events
b. Mission support for OSPP designated Launch and Recovery Windows

6.2.1 UNITeS NSS Service IT Support Locations

The NSS equipment points of presence are at all NASA Centers, HQ, GSFC's White Sands Complex (WSC) and the Jet Propulsion Laboratory (JPL). NSS IT personnel are located at MSFC, HQ and KSC. Therefore personnel from MSFC, HQ and KSC may travel to any of the NASA Centers, WSC or JPL in support of equipment maintenance.

The central office of record for the NSS COMSEC equipment is KSC.

In the future, it is expected that the NICS contractor will cross train and clear their center staff such that additional contractors are available to support the NSS Service IT Support team in the

event of additional needs as defined by OSPP, e.g. additional Mission Support at JSC or KSC, Hurricane Events etc.

6.2.2 UNITeS NSS IT Support Work Load Indicators

The UNITeS contractor provides the people and equipment (e.g. networking and desktops) to interface to government provided equipment to operate this network as follows:

a. MSFC – Ten (10) TS/SCI/COMSEC cleared engineers
b. HQ – Two (2) TS/SCI/COMSEC cleared engineers
c. KSC – Two (2) TS/SCI COMSEC cleared engineers
d. MSFC – One (1) TS/SCI/COMSEC cleared COMSEC Account Manager (CAM) specialist

6.3 UNITES DIGITAL TELEVISION (DTV) ENGINEERING SERVICE

NASA-wide coordination of Digital Television (DTV) implementation is the primary role of the DTV Engineering Service, UNITeS provides engineering support to NASA for this service. Standards development, best practices and strategic planning are a major function. The DTV NASA technical lead and the UNITeS engineers, function as technical consultant to all NASA Centers, Headquarters, and major NASA programs for design and implementation of DTV technologies and capabilities.

The DTV Engineering Service has the following responsibilities:

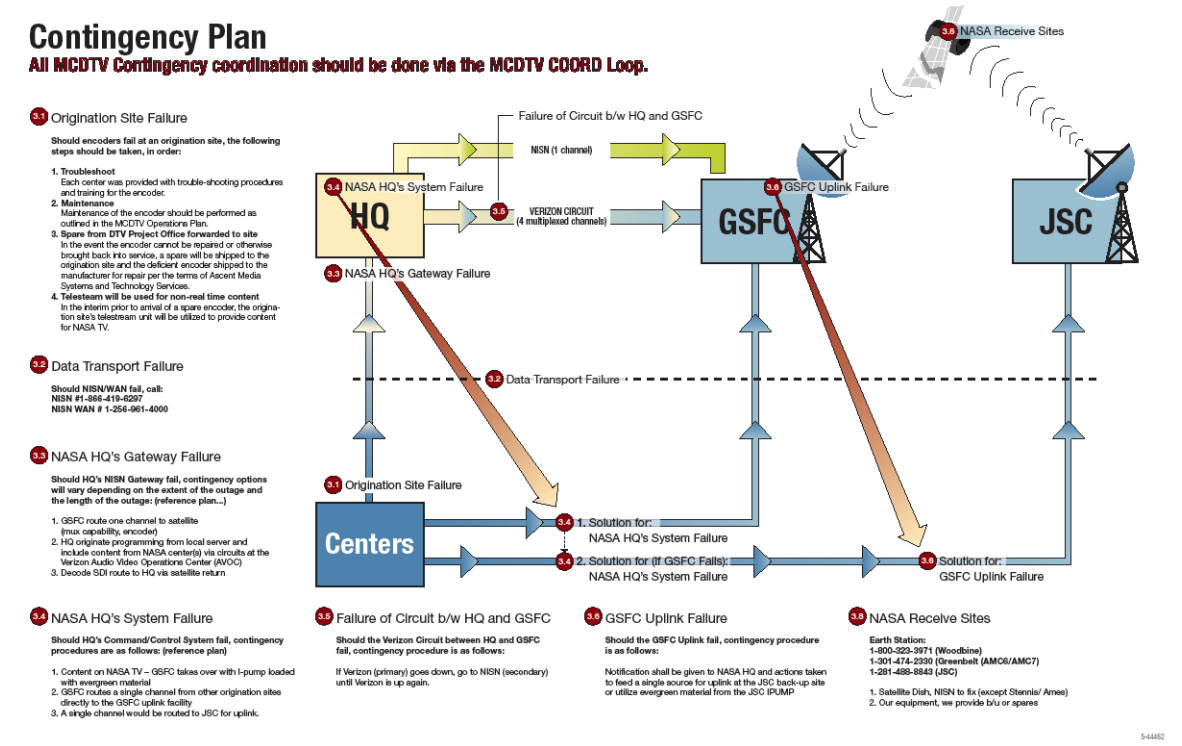
a. Determining NASA DTV requirements
b. Developing transition and implementation plans
c. Operating a DTV test facility to assist in setting NASA DTV standards
d. Technical coordination with the television broadcast industry
e. Acting as an engineering and implementation consultant to all NASA centers and major programs
f. General coordination of NASA DTV Implementation
g. Organization and participation in technical working groups, both NASA and industry

The DTV Engineering Service group is the Agency expert's in digital television, serving as the coordination group to schedule and implement the transition from analog to digital television and implementation of High Definition Television (HDTV) capabilities. The group has developed transition and detailed implementation plans that take into account NASA requirements and the broadcast industry transition to digital. The plans are updated as required to reflect Agency and industry changes. The group sets NASA DTV standards by operating a test facility that allows various operational concepts to be validated against user requirements. The following documents provide more insight into the engineering services provided:

a. NASA STD 2818 Digital Television Standard for NASA

b. MCDTV Operations Plan
c. 2008 Testing NASA DTV
d. Fly Away System

The following depicts the NASA MCDTV System, the transport is provided as a NISN customer service:



The DTV Engineering Service group, through technical coordination of the DTV test facility and participation in industry technical working groups, has developed an expertise within DTV. This expertise is used as a pool of technical talent to assist all NASA centers in engineering and implementation of their DTV systems.

6.3.1 Major Activities

Major activities of the DTV Engineering Service group within the past several years include:

a. Key technical support to Shuttle Launch and Landing video documentation system during aftermath of Columbia Accident
b. Sensor Lead for the WB-57 Ascent Video Experiment, a Return-to-Flight project responding to the Columbia Accident Investigation Board, providing a capability to image the shuttle from high altitude during launch.
c. Responsible for the upgrade of Kennedy Space Center's Media Center to HDTV.

d. Engineered and implemented the transition of NASA Television from a single analog channel to a multi-channel digital system.
e. Supported the Principal Investigator for a Development Test Objective on the International Space Station that enabled the first ever live HDTV broadcast from an orbiting space craft.
f. Engineered the transition of the Shuttle Program's analog video satellite services to a more capable digital system.
g. Ongoing activities of the DTV Program include:
h. Engineering and maintenance of the Multi-Channel NASA TV System.
i. Coordinate with various commercial manufacturers to develop high performance HDTV acquisition, processing, production, and encoding equipment to meet the requirements of the Constellation Program.
j. Maintenance and deployment as required of an Agency HDTV portable production system, referred to as an HDTV "Fly-away" system.
k. Continued support of International Space Station projects to add HDTV capabilities to the station.
l. Support program related imagery working groups, such as the Constellation Imagery Working Group and ISS Imagery Working Group.
m. Maintain and update NASA Standard 2818 and create future standards as required to ensure continuity of digital television and video related activities across the Agency.
n. Lead the Agency transition to complete HDTV production and distribution capability.
o. Support management and leadership of the NASA DTV Working Group, DTV and NASA TV Control Boards, and the Consultative Committee for Space Data Systems Motion Imagery and Applications Working Group.

6.3.2 Work Load Indicators

UNITeS support for DTV Engineering Service consist of two (2) engineers. The table below depicts the approximate direct labor hours expended in FY07 and FY08 for the DTV Engineering Service provided by UNITeS for DTV.

		FY08	FY09
UNITeS PWS	PWS Title	Approximate Total Hrs	Approximate Total Hrs
3.2	Digital TV	5,000	5,300

6.3.3 Applicable Documents

Located at: NASA Standards, http://standards.nasa.gov

a. NASA STD 2818 Digital Television Standard for NASA

Located at NICS, Other Documents, B&H Applicable Documents:

http://ec.msfc.nasa.gov/apt/portal_acqDetails.php?acqNum=1

a. *MCDTV Operations Plan,* (MCDTV_OPSPLAN_V1_2_July24_2007.doc)
b. *2008 Testing NASA DTV*, (2008_Lab_Testing_1.doc)
c. *Fly Away System*, (Fly_Away_Drawings.pdf)