★**CYBERSPACE SUPPORT CAREER FIELD (3D)**
(Changed 31 Oct 20)

Introduction

The Cyberspace Operations specialty (3D0) encompasses: Knowledge Management, Cyber Systems Operations, Cyber Surety and Computer Systems Programming. Included are activities to: plan, coordinate, share, and control an organization's data and information assets and manage technologies to capture, organize, and store tacit and explicit knowledge; administering server-based networked systems, distributed applications, network storage, messaging, and application monitoring required to provision, sustain, operate and integrate cyber networked systems and applications; identifying and managing Information Technology (IT) and Telecommunications resources to monitor, evaluate and maintain systems, policy and procedures to protect clients, networks, data/voice systems and databases from unauthorized activity; and analyzing, coding, testing and managing the design, development, maintenance, testing, configuration management, and documentation of application software systems, client-server, and web-enabled software and relational database systems critical to warfighting capabilities.

The Cyberspace Systems specialty (3D1) encompasses: Client Systems, Cyber Transport, Radio Frequency (RF) Transmission Systems, Spectrum Operations, and Cable and Antenna Systems. Included are activities to: deploy, sustain, troubleshoot and repair standard voice, data, video network and cryptographic client devices; perform, coordinate, integrate and supervise network design, configuration, operation, defense, restoration, and improvements; sustain, troubleshoot and repair standard radio frequency wireless, line-of-sight, beyond line-of-sight, and encryption transmission devices; analyze electromagnetic spectrum requirements and request frequencies to support terrestrial, aircraft, and space systems and coordinate radio, radar, land, and other electromagnetic radiating or receiving requirements; ground and space based satellite, wideband communications, telemetry, and instrumentation systems, ground-to-air transmitters, receivers and transceivers; and, provide command and control (C2) capabilities through installation, maintenance, fault isolation, and reconstitution of fixed cable and wireless distribution systems, local area networks (LAN), and wide area networks (WAN) in support of tactical and strategic operations.

These Air Force Specialty Code description incorporate the use of Defense Cyberspace Workforce Framework (DCWF) Codes to tie the specialty description to the framework. The DCWF was developed by the National Institute of Standards and Technology (NIST) and the DoD to establish a common lexicon and model for all cyber work. The DCWF will universalize training and education between academia, industry and military. It will also enable talent management by ensuring the right Airmen, for the right assignment, at the right time.

CEM Code 3D100
AFSC 3D190, Superintendent

CYBERSPACE SUPPORT
(Changed 31 Oct 19)

1. **Specialty Summary.** Manages cyberspace system analysis and design, programming, systems operation and maintenance, resource management and security management. Directs activities for installing, maintaining, repairing, overhauling, deploying, and modifying cyberspace systems and equipment platforms. In addition, manages and directs network operations in garrison and at deployed locations by performing duties to develop, sustain, and enhance network and electromagnetic capabilities to defend national interests from attack. Ensures personnel are trained, equipped, and available to perform the assigned mission. Conducts career field development and mentoring for subordinate cyberspace support personnel. Introduces Airmen to career field path and steers growth to feed into the cyberspace deliberate development program. Related DoD Occupational Subgroup: 240300, and 270500.

2. **Duties and Responsibilities:**
2.1. Plans and organizes cyberspace support activities. Plans and supervises system installation and evaluates facilities layout and performance standards. Designs and develops organizational structures and determines equipment, training, and supplies required for systems implementation and support. Interacts with customers to promote customer satisfaction. Establishes tactics, techniques, and procedures. Evaluates operational readiness of communications equipment, network devices, sensors, intrusion detection, and related support equipment.
2.2. Directs activities responsible for system analysis and design, programming, operations and maintenance, security, systems management, technical support, plans, implementation, and resource management. Implements and interprets policies, directives, and procedures.
2.3. Establishes training requirements. Establishes training programs to meet local knowledge and certification requirements and to enhance professional awareness of technology.
2.4. Directs maintenance activities. Directs personnel employed in siting, deploying, inspecting, adjusting, removing, replacing, repairing, operating, and defending communications systems and related equipment. Prepares and analyzes reports encompassing siting, deploying, maintaining, installing, repairing, and removing communications systems and related equipment. Coordinates activities and resolves common problems. Directs overhaul and repair of communications systems and related equipment. Establishes local maintenance procedures and policies. Ensures work standards are maintained. Determines extent and economy of repair, including disposition of malfunctioning equipment.
2.5. Inspects and evaluates maintenance activities for compliance with directives. Evaluates, rates, and prepares reports. Recommends and implements corrective action for improved methods and procedures. Evaluates effectiveness of equipment usage, systems performance, customer service, supplies, system scheduling, processing, and maintenance.
2.6. Plans, programs, and develops budget inputs to ensure resource availability for operational and training requirements.
2.7. Manages plans, implementation and development functions. Helps functional users define requirements. Recommends automated methods to enhance resource use. Supervises functional user requirements translation into automated systems capabilities. Organizes teams that use methodologies to meet mission requirements. Supervises test and evaluation efforts to determine performance. Organizes and participates in mission implementation and conversion. Ensures continued interface between functional users, and programming and operations personnel for implemented systems. Ensures compliance with standards for systems documentation.
2.8. Conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. **Specialty Qualifications:**
3.1. Knowledge. Knowledge is mandatory of: techniques and procedures of systems analysis and design; project management, communications-computer processing; system operation and maintenance; system and equipment capability, capacity, and logic; personnel and equipment performance measurement; awards programs and manpower and organization; security, administrative contract, training, resource, records, publications, deployment, logistics, and base/unit functional management.
3.2. Education. Not used.
3.3. Training. For award of AFSC 3D190, completion of E6ACW3DX9X 00AA Cyberspace 9-level Course is required.
3.4. Experience. For award of AFSC 3D190, qualification in and possession of AFSC 3D071/72/73/74 or 3D171/72/73/74/77 is mandatory. Also, experience is mandatory in directing functions such as installing, maintaining, operating, repairing, or modifying the various cyberspace systems, software development, cyber security, or resource management as related to the feeder specialties.
3.5. Other. For award and retention of this AFSC:
3.5.1. Completion of current Tier 3 (T3) background investigation according to AFMAN 16-1405, *Personnel Security Program Management*, is mandatory.
3.5.2. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer*

Security.
3.5.3. Specialty requires routine access to Tier 3 (T3) information, systems or similar classified environments.

AFSC 3D071, Craftsman
AFSC 3D051, Journeyman
AFSC 3D031, Apprentice
AFSC 3D011, Helper

★**KNOWLEDGE MANAGEMENT**
(Changed 31 Oct 20)

1. **Specialty Summary.** Develop, govern, and monitor processes, technologies, and practices that support organizations to identify, capture, document, organize, and employ information in both fixed and deployed environments. These information assets comprise of raw data, documents, practices, policies, and individual expertise. Core competencies of Knowledge Managers include: professional networking, social collaboration, Communities of Practice (CoP), enterprise information systems technology, business continuity, cross-functional data sharing, and process-improvement. Related DoD Occupational Subgroup: 151000.

2. ★**Duties and Responsibilities:**
2.1. Manages the overall process for organizations to plan, coordinate, manage, share, and control information. Identifies and analyzes data, information, and knowledge requirements to facilitate discovery and dissemination of decision-quality information. Leverages the interaction of people, processes, and enterprise technologies to capture, store, organize, share, and control tacit and explicit knowledge. Develops an understanding of the needs and requirements of information end-users. Leverages continuous process improvement techniques to improve mission and business processes, enhancing access to relevant cross- functional information in a collaborative, timely, and contextual manner. Promotes organizational information as a reusable, shared, protected, consistent, and compliant resource. Manages and enforces use of metadata, enabling data to be accessed, tagged, and searched regardless of physical location, media, source, owner, or other defining characteristics. Monitors and reports the usage of knowledge management assets and resources. Assists and educates users on authoritative data sources, data services, and presentation tools to meet organizational objectives. Plan and manage the delivery of knowledge management projects. [DCWF Code-431]
2.2. Assists organizations with meeting statutory records management requirements, to include training, policies, and technologies used to identify, organize, protect, share, archive, and dispose of official government records. Operates and manages records, information, management systems, and records staging facilities for long-term and permanent records. Provides assistance and training with Privacy Act, Freedom of Information Act, and Civil Liberties programs.
2.3. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs, and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency, and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]
2.4. Conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code – 511, 521, 531, 541]
2.5. ★Develops and writes new or modifies existing specialized utility programs (scripts) following software assurance best practices. Tests specialized utility programs (scripts) to ensure they meet intended performance targets. Deploys specialized utility programs (scripts) to automate the deployment of software packages or simplify the collection of systems/software data. [DCWF Code – 621]

3. **Specialty Qualifications:**
3.1. Knowledge. Knowledge is mandatory of: planning and coordinating the complete life-cycle of organizational data and information assets, including enterprise information management, technologies, information security, and knowledge operations.
3.2. Education. For entry into this specialty, completion of high school or general education development equivalency is mandatory. Additional courses in business, mathematics, computer science, and information systems are desirable.
3.3. Training. For award of AFSC 3D031, completion of Knowledge Management initial skills course is mandatory.
3.4. Experience. The following experience is mandatory for award of the AFSC indicated:
3.4.1. 3D051. Qualification in and possession of AFSC 3D031. Experience or knowledge of collaboration/web service applications; information architectures; records management; and knowledge management principles.
3.4.2. 3D071. Qualification in and possession of AFSC 3D051. Experience performing or supervising knowledge management planning functions such as applying knowledge management principles, solutions, and technologies to improve the effectiveness and efficiency of Air Force organizations.
3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty: See attachment 4 for entry requirements.

3.5.2. <u>For award and retention of these AFSCs:</u>

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.3. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Ground Transportation* is desired.

AFSC 3D072, Craftsman
AFSC 3D052, Journeyman
AFSC 3D032, Apprentice
AFSC 3D012, Helper

★**CYBER SYSTEMS OPERATIONS**
(Changed 31 Oct 20)

1. **Specialty Summary.** Installs, supports, and maintains server operating systems or other computer systems and the software applications pertinent to its operation, while also ensuring current defensive mechanisms are in place. Responds to service outages and interruptions to network operations. Administers server-based networked systems, distributed applications, network storage, messaging, and application monitoring required to provision, sustain, operate, and integrate cyber networked systems and applications in garrison and at deployed locations. Core competencies include: server operating systems, database administration, web technologies, systems- related project management, and supervising cyber systems. Supports identification and remediation of vulnerabilities while enhancing capabilities within cyber environments to achieve desired affects. Related DoD Occupational Subgroup: 153100.

2. ★**Duties and Responsibilities:**
2.1. Defends, protects, and secures mission networking environments and devices. Provides networked application resources by designing, configuring, installing, and managing data services, operating system, and server applications. Provides directory services utilizing dynamically-assigned internet protocol (IP) addresses, domain name server (DNS), network storage devices, and electronic messaging resources. Manages secure authentication methods utilizing public key infrastructure (PKI) technologies and procedures. Standardizes user privileges and system settings using automated deployment tools such as Group Policy Management Console (GMPC) and System Management Server (SMS). Manage accounts, network rights, and access to systems and equipment according to standards, business rules, and needs. Implements server and special mission system security fixes, operating system patches, and antivirus software. Develops, tests, and implements local restoral and contingency operations plans. Processes and reviews C4 systems requirement documentation, telecommunication service requests, status of acquisition messages, and telecommunication service orders. Performs strategic and budget planning for networks. [DCWF Code - 441, 451]
2.2. Performs user accounts management and standardizes systems settings using automated deployment tools. Manages physical, virtual, and cloud-based server/client hardware. Performs system-wide backups and data recovery. Ensures continuing systems operability by providing ongoing optimization and problem solving support. [DCWF Code - 441, 451]
2.3. Performs system resource management, to include load and capacity planning and balance. Creates, administers, and audits system accounts. Performs system-wide backups and data recovery. Ensures continuing systems operability by providing ongoing optimization and problem solving support. Applies computer security policies to safeguard systems and information. Categorizes, isolates, and resolves system problems. Performs fault recovery by validating, isolating, correcting faults, and verifying service restoral with customers. Processes, documents, and coordinates resolution of trouble calls from lower support echelons. Processes scheduled and authorized outages. Submits outage reports in response to unscheduled outages. [DCWF Code - 441, 451]
2.4. Utilizes enterprise patching tools to implement security updates and patches to include: Information Assurance Vulnerability Assessments, C4 Notice to Airman, Time Compliance Network Orders, Time Compliance Technical Order, operating system patches, and antivirus software updates. Implements and enforces national, DoD, and Air Force security policies and directives. Performs proactive security functions to deter, detect, isolate, contain, and recover from information system and network security intrusions. Performs system sanitation resulting from classified message incidents and classified file incidents. [DCWF Code - 441, 451, 461]
2.5. Supports information warfare operations within strictly controlled parameters and provides real-time intrusion detection and firewall protection for all networked resources. Researches latest system threats to develop and test tactics, techniques, and procedures (TTPs) for defensive information operations. Employs TTPs on Air Force and DoD computer networks to defend against hostile information operations. Analyzes risks and/or vulnerabilities and takes corrective action to mitigate or remove them. [DCWF Code - 511, 521, 541]
2.6. Reviews and implements C4 systems requirements. Performs strategic and budget planning for systems hardware and software. Coordinates and implements system service level agreements and memoranda of understanding with user agencies.
2.7. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]
2.8. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control,

patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

2.9. Performs risk management framework security determinations of fixed, deployed, and mobile information systems (IS) and telecommunications resources to monitor, evaluate, and maintain systems, policy, and procedures to protect clients, networks, data/voice systems, and databases from unauthorized activity. Identifies potential threats, administers, and manages resolution of Communications Security (COMSEC) incidents. [DCWF Code - 461, 722]

2.10. ★Develops and writes new or modifies existing specialized utility programs (scripts) following software assurance best practices. Tests specialized utility programs (scripts) to ensure they meet intended performance targets. Deploys specialized utility programs (scripts) to automate the deployment of software packages or simplify the collection of systems/software data. [DCWF Code – 621]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge is mandatory of cyber systems elements: capabilities, functions, and technical methods for system operations.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses or certifications in computer and information systems technology are desirable. Any network or computing commercial certification is desirable.

3.3 Training. For award of AFSC, completion of Cyber System s Operations initial skills course is mandatory.

3.3.   Experience. The following experience is mandatory for award of the AFSC indicated:

3.3.1. 3D052. Qualification in and possession of AFSC 3D032. Experience in functions such as system operations, multi-user technical support, system restoral, resource counting, or security.

3.3.2. 3D072. Qualification in and possession of AFSC 3D052. Experience supervising one of the following functions: analysis of system failure and restoral, operations, command and control systems support, system administration, or resource and project management.

3.5.   Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty, see attachment 4 for entry requirements.

3.5.2. <u>For award and retention of this AFSC:</u>

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.3. Specialty routinely requires work in the networking environment.

3.5.3.1.   Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program.*

3.5.2.4. Completion of a current Tier 5 (T5) background investigation according to AFMAN 16-1405, *Personnel Security Program Management*, is mandatory.

3.5.2.5. Must maintain a T5 clearance for retention of this AFSC.

3.5.2.6. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Ground Transportation* is desired.

NOTE: Award of entry level without a completed T5 Investigation is authorized provided an interim Top Secret clearance has been granted according to AFMAN 16-1405.

AFSC 3D073, Craftsman
AFSC 3D053, Journeyman
AFSC 3D033, Apprentice
AFSC 3D013, Helper

★CYBER SURETY
(Changed 31 Oct 20)

1. Specialty Summary. Performs risk management framework security determinations of fixed, deployed, and mobile information systems (IS) and telecommunications resources to monitor, evaluate, and maintain systems, policy, and procedures to protect clients, networks, data/voice systems, and databases from unauthorized activity. Identifies potential threats and manages resolution of communications security incidents. Enforces national, DoD, and Air Force security policies and directives to ensure Confidentiality, Integrity, and Availability (CIA) of IS resources. Administers and manages the overall cybersecurity program to include Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC) programs. Related DoD Occupational Subgroup: 153000.

2. ★Duties and Responsibilities:

2.1. Conducts cybersecurity risk management framework assessments; ensures enterprise cybersecurity policies fully support all legal and regulatory requirements and ensures cybersecurity policies are applied in new and existing IS resources. Identifies cybersecurity weaknesses and provides recommendations for improvement. Monitors enterprise cybersecurity policy compliance and provides recommendations for effective implementation of IS security controls. Defends, protects, and secures mission networking environments and devices. Provides networked application resources by designing, configuring, installing, and managing data services, operating system, and server applications. [DCWF Code - 541, 612]

2.2. Evaluates and assists IS risk management activities. Makes periodic evaluation and assistance visits, notes discrepancies, and recommends corrective actions. Audits and enforces the compliance of cybersecurity procedures and investigates security-related incidents to include COMSEC incidents, classified message incidents, classified file incidents, classified data spillage, unauthorized device connections, and unauthorized network access. Develops and manages the cybersecurity program and monitors emerging security technologies and industry best practices while providing guidance to unit-level Information Assurance (IA) Officers. Employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of government information processed by AF IS's. [DCWF Code - 541, 612]

2.3. Responsible for cybersecurity risk management of national security systems during all phases of the IS life cycle through remanence security. [DCWF Code - 722]

2.4. Integrates risk management framework tools with other IS functions to protect and defend IS resources. Advises cyber systems operations personnel and system administrators on known vulnerabilities and assists in developing mitigation and remediation strategies. Provides CIA by verifying cybersecurity controls are implemented in accordance with DoD and Air Force standards. Ensures appropriate administrative, physical, and technical safeguards are incorporated into all new and existing IS resources and protects IS resources from malicious activity. [DCWF Code - 541, 612]

2.5. Performs COMSEC management duties in accordance with national and DoD directives. Maintains accounting for all required physical and electronic cryptographic material. Issues cryptographic material to units COMSEC Responsible Officer (CRO). Provides guidance and training to appointed primary/alternate CRO. Conducts inspections to ensure COMSEC material is properly maintained and investigates and reports all COMSEC related incidents. [DCWF Code - 723]

2.6. Performs TEMPEST duties in accordance with national and DoD TEMPEST standards. Denies unauthorized access to classified, and in some instances, unclassified information via compromising emanations within a controlled space through effective countermeasure application. Ensures all systems and devices comply with national and DoD EMSEC standards. Inspects classified work areas, provides guidelines and training, maintains area certifications, determines countermeasures; advises commanders on vulnerabilities, threats, and risks; and recommends practical courses of action. [DCWF Code - 722]

2.7. Responsible for oversight or management of installation cybersecurity awareness programs. Promotes cybersecurity awareness through periodic training, visual aids, newsletters, or other dissemination methods in accordance with organizational requirements.

2.8. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs, and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]

2.9. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission

201

mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

2.10. ★Develops and writes new or modifies existing specialized utility programs (scripts) following software assurance best practices. Tests specialized utility programs (scripts) to ensure they meet intended performance targets. Deploys specialized utility programs (scripts) to automate the deployment of software packages or simplify the collection of systems/software data. [DCWF Code – 621]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge is mandatory of: IS resources; capabilities, functions and technical methods for IS operations; organization and functions of networked IS resources; communications-computer flows, operations and logic of electromechanical and electronics

IS and their components, techniques for solving IS operations problems; and IS resources security procedures and programs including Internet Protocols.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses or certifications in computer and information systems technology are desirable. Any network or computing commercial certification is desirable.

3.3. Training. For award of AFSC 3D033, completion of Cyber Surety initial skills course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D053. Qualification in and possession of AFSC 3D033. Experience performing cybersecurity functions and/or activities.

3.4.2. 3D073. Qualification in and possession of AFSC 3D053. Experience supervising cybersecurity functions and/or activities or resource and project management.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty, see attachment 4 for entry requirements.

3.5.2. For award and retention of this AFSC:

3.5.2.1. Individual must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.2.2. Specialty routinely requires work in the networking environment.

3.5.2.3. Must attain and maintain a minimum Information Assurance Management Level I certification IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program.*

3.5.2.4. Specialty requires routine access to Tier 5 (T5) information, systems or similar classified environments.

3.5.2.5. Completion of a current Tier 5 (T5) background investigation according to AFMAN 16-1405, *Personnel Security Program Management,* is mandatory.

3.5.2.6. Must maintain a T5 clearance for retention of this AFSC.

NOTE: Award of the entry level without a completed T5 Investigation is authorized provided an interim Top Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D074, Craftsman
AFSC 3D054, Journeyman
AFSC 3D034, Apprentice
AFSC 3D014, Helper

★**COMPUTER SYSTEMS PROGRAMMING**
(Changed 31 Oct 20)

1.   **Specialty Summary.** Supervises, teams, and performs as computer analyst, coder, tester, product manager, product designer, product developer, maintenance, testing, configuration management, and documentation of application software systems, client-server, and web-enabled software and relational database systems of customer-defined software and software-intensive weapon systems critical to warfighting capabilities. Related DoD Occupational Subgroup: 153200.

2.   ★**Duties and Responsibilities:**
2.1. ★Develops standardized tools and interfaces in accordance with Air Force Network Operations guidance, DoD directives and standards for security and interoperability to transform raw data into actionable C2 information. Develops and implements policy to enable effective information discovery, indexing, storage, life-cycle management, retrieval, and sharing in a collaborative enterprise information environment. Harnesses capabilities of systems designed to collect, store, retrieve, process, and display data to ensure information dominance. Develops and administers databases, data management systems, and/or data processes that allow for the storage, query, and utilization of data. Analyzes and plans for anticipated changes in data capacity requirements. Implements data management standards, requirements, and specifications. Installs and configures database management systems and software. Maintains database management systems software. Monitors and maintains databases to ensure optimal performance. Performs backup and recovery of databases to ensure data integrity and availability. Performs configuration management, problem management, capacity management, and financial management for databases and data management systems. [DCWF Code – 421, 422/621/622/632]
2.2. ★Software Developer/Secure Software Assessor. Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. Works on the development phases of the system development lifecycle. Designs, develops, test, and evaluates information systems throughout the systems development lifecycle. Researches problems and breaks them into deliverable software iterations. Exhibits strong communication skills/ works in an individual- or pair-programming environment. Uses Lean, Extreme Programming, User Centered Design and Agile methodologies. [DCWF Code – 621/622/632]
2.3. ★Product Designer. Makes daily product decisions, works on a collaborative team, pairs with team members, and helps ensure user satisfaction using Lean and Agile methodologies. Understands user needs and solves the right problems to deliver new or improved products and services that meet the needs of the Air Force. Creates intuitive, innovative, and effective products that military operators' desire, through learning and understanding of users' needs, behaviors, and emotions to yield insights that inform product strategy and guide the design of the software and systems. Develops complex, software systems that scale globally to meet the demands of warfighters across multiple domains, through the full range of development activities, to include web application development, platform development, mobile application development, distributed and parallel systems, machine learning, information retrieval, natural language processing, networking, and/or security software development. [DCWF Code – 621]
2.4. ★Product Manager. Defines and prioritizes product features using Agile/Lean product development practices. Works with the project team, leadership, stakeholders, and other PMs to progress the goal of shipping the right product to users. Ensures that the product is successful in terms of user value, stakeholder value, and organizational business goals. Architects the future of products by bridging development and business through the management of a product's full lifecycle, from strategic planning to development and launch, in order to generate value for combat capabilities. [DCWF Code – 621]
2.5. ★Data/Database Analyst/Specialist. Develops, administers, and secures databases, data management systems, and/or data processes for the storage, query, and utilization of data. Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. Locates patterns in large data sets using computer science techniques to help team members with different levels of understanding and expertise to make data driven business decisions that increase effectiveness or efficiency of operational forces. [DCWF Code – 421/422]
2.6. ★Ensures compliance with DoD directives and standards for security and interoperability. Protects operating systems, application software, files, and databases from unauthorized access to sensitive information, or misuse of communication-computer resources.
2.7. ★Software Developer. Determines, analyzes, and develops requirements for software systems through interpreting standards, specifications, and user needs as a system analyst. Determines, designs, and develops data requirements, database structure, process flow, systematic procedures, algorithms, and file structures to implement and maintain software systems using software engineering techniques. Works with systems using software methodologies such as distributed processing, systems networking, advanced information storage and retrieval, and management techniques. Determines and recommends the most reasonable approach in designing new systems or modifying existing systems. Develops and maintains system specifications. Conducts and participates in system reviews and technical interchanges. Selects appropriate software development tools. Explores commercial off-the-shelf options to satisfy user requirements. Researches problems and breaks them into deliverable software iterations. Exhibits strong communication skills/ works in an individual- or pair-programming environment. Uses Lean, Extreme Programming, User Centered Design and Agile methodologies.

[DCWF Code - 632, 641]

2.8. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs, and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]

2.9. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge is mandatory of system capabilities, limitations, and programming logic; techniques and procedures of systems analysis and design; related information processing devices and systems; software methodologies; methods of editing input and output data; configuration management techniques; security practices; customer relations; application of mathematical and analytical concepts to process problems; and computer program editing and testing techniques.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in algebra, geometry, computer science and computer programming is desirable. Any network or computing commercial certification is desirable.

3.3. Training. For award of AFSC 3D034, completion of a Computer Systems Programming initial skills course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D054. Qualification in and possession of AFSC 3D034. Experience performing programming functions such as designing, coding, testing, or documenting software.

3.4.2. 3D074. Qualification in and possession of AFSC 3D054. Experience performing or supervising one of the functions of programming, such as preparing system requirements, developing high-level or detailed designs, translating designs into code, testing, configuration management, or project management.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty

3.5.1.1. See attachment 4 for additional entry requirements.

3.5.2. For award and retention of this AFSC:

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.2.2. Specialty requires routine access to Tier 5 (T5) information, systems or similar classified environments.

3.5.2.3. Completion of a current T5 background investigation according to AFMAN 16-1405, *Personnel Security Program Management,* is mandatory.

3.5.2.4. Must maintain a T5 clearance for retention of this AFSC.

NOTE: Award of entry level without a completed T5 Investigation is authorized provided an interim Top Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D171, Craftsman
AFSC 3D151, Journeyman
AFSC 3D131, Apprentice
AFSC 3D111, Helper

★**CLIENT SYSTEMS**
(Changed 31 Oct 20)

1. **Specialty Summary.** Deploys, sustains, troubleshoots and repairs standard voice, data, video network and cryptographic client devices in fixed and deployed environments. Sustains and operates systems through effective troubleshooting, repair, and system performance analysis. Manages client user accounts and organizational client device accounts. Related DoD Occupational Subgroup: 110000 and 115000.

2. ★**Duties and Responsibilities:**
2.1. Performs client-level information technology support functions. Manages hardware and software. Performs configuration, management, and troubleshooting. Removes and replaces components and peripherals to restore system operation. Installs and configures software operating systems and applications. Provides service to end-users for operation, restoration, and configuration of information systems. Reports security incidents and executes corrective security procedures. Manages client user accounts. [DCWF Code - 411, 451]
2.2. Performs client-level voice network functions. Manages client hardware and software. Performs configuration, management to include adds, moves, changes and troubleshooting between the wall outlet to the client device. Plans, schedules, and implements installation and maintenance functions associated with voice systems. Removes and replaces telephone instruments. Reports security incidents and executes corrective security procedures. [DCWF Code - 411, 451]
2.3. Performs client-level Personal Wireless Communication Systems (PWCS) functions with the exception of Land Mobile Radios (LMRs). Manages hardware, software and Controlled Cryptographic Items (CCI). Performs configuration, management, and troubleshooting. Plans, schedules, and implements installation and maintenance functions associated with PWCS. Removes and replaces components and peripherals to restore system operation. Reports security incidents and executes corrective security procedures. [DCWF Code - 411]
2.4. ★Plans, organizes and directs sustainment activities. Establishes work standards, methods and controls for preventative, scheduled, and unscheduled maintenance actions. Determines extent and economy of repair of malfunctioning equipment. Ensures compliance with technical data, instructions, and work standards. Develops and enforces safety standards. Interprets malfunctions and prescribes corrective action. Serves on, or directs inspection teams organized to evaluate base or command sustainment programs. Manages, or performs research and development projects for assigned systems. Coordinates and documents repairs. Manages, administers, controls, and evaluates contracts. Manages organizational client device accounts with the exception of LMR devices.
2.5. ★ Develops and writes new or modifies existing specialized utility programs (scripts) following software assurance best practices. Tests specialized utility programs (scripts) to ensure they meet intended performance targets. Deploys specialized utility programs (scripts) to automate the deployment of software packages or simplify the collection of systems/software data.
2.6. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]
2.7. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. **Specialty Qualifications:**
3.1. Knowledge. Knowledge of: IT fundamentals, test equipment, special tools, maintenance, management, and security practices is mandatory.
3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in mathematics, computer science, computer principles, or information technology is desirable. Any network or computing commercial certification is desirable.
3.3. Training. For award of AFSC 3D131, completion of Client Systems initial skills course is mandatory.
3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D151. Qualification in and possession of AFSC 3D131. Also, experience performing functions such as client systems support.

3.4.2. 3D171. Qualification in and possession of AFSC 3D151. Also, experience performing or supervising functions such as client systems support and management of information systems.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty, see attachment 4 for additional entry requirements.

3.5.2. For entry, award, and retention of this specialty:

3.5.2.1. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Vehicle Operations* is desired.

3.5.2.2. Normal color vision as defined in AFI 48-123, *Medical Examinations and Standards.*

NOTE: Color vision requirement does not apply to personnel awarded AFSC 3D1X1 as of 30 Apr 2012 or before which includes those in the recruiting pipeline and scheduled for or attending the 3-skill level technical training course as of that date.

3.5.3. For award and retention of this AFSC:

3.5.3.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.3.2. Specialty routinely requires work in the networking environment.

3.5.3.2.1. Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and DoD 8570.01-M *Information Assurance Workforce Improvement Program.*

3.5.3.3. Specialty requires routine access to Tier 3 (T3) information, systems or similar classified environments.

3.5.4. For award and retention of AFSCs 3D151/71:

3.5.4.1. Completion of a T3 background investigation according to AFMAN 16-1405, *Personnel Security Program Management.*

NOTE: Award of the entry level without a completed T3 Investigation is authorized provided an interim Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D172, Craftsman
AFSC 3D152, Journeyman
AFSC 3D132, Apprentice
AFSC 3D112, Helper

★**CYBER TRANSPORT SYSTEMS**
(Changed 31 Oct 20)

1. **Specialty Summary.** Deploys, sustains, troubleshoots and repairs standard voice, data and video network infrastructure systems, IP detection systems and cryptographic equipment. Performs, coordinates, integrates and supervises network design, configuration, operation, defense, restoration, and improvements. Analyzes capabilities and performance, identifies problems, and takes corrective action. Fabricates, terminates, and interconnects wiring and associated network infrastructure devices. Related DoD Occupational Subgroups: 115000 and 162200.

2. **Duties and Responsibilities:**
2.1. Provides voice, data and video services. Installs, upgrades, replaces, configures and maintains systems/circuits/IP-based intrusion detection/long haul communications systems that access military, federal and commercial networks. Manages infrastructure devices and systems using the latest approved software tools. [DCWF Code - 441]
2.2. Deploys and operates expeditionary communications systems. Uses agile logistics support channels to sustain continuous network operations. Removes, repairs and replaces assemblies and subassemblies to optimally sustain voice, data and video networks. [DCWF Code - 441]
2.3. Establishes restoral and job priorities, maintains, tests, troubleshoots, and repairs voice and network systems equipment and circuits utilizing tools and test equipment. Isolates malfunctions using diagnostic software, technical data, block diagrams, voltage and waveform measurements, and other tests requiring specialized test equipment. [DCWF Code - 521]
2.4. Monitors performance of systems and circuits. Coordinates with coalition forces, DoD agencies and other service providers to analyze and isolate performance faults and implement corrective actions. Checks equipment for serviceability and performs preventive maintenance. Isolates faults by coordinating with commercial service providers and depots to test system components and assemblies. [DCWF Code - 521]
2.5. Maintains and administers voice, network and circuit databases, records and forms. Interprets sketches and layout drawings for placement of distribution systems. Coordinates request for service orders. Reviews, recommends, and implements changes to communications-computer systems installations records (CSIR), technical data, engineering drawings, and equipment wiring diagrams. Updates and verifies entries on system, facility, maintenance, and inspection records. Initiates, tracks, and maintains shipping, receiving, supply, and equipment documents. [DCWF Code - 441, 521]
2.6. Conducts periodic inspections of systems installations and repair activities. Interprets inspection reports and implements corrective actions, documents inspection and maintenance actions.
2.7. Reviews and maintains operational measurement reports and analyzes network utilization. Ensures equipment and components meet installation practice technical order and accepted commercial installation specifications. [DCWF Code - 441]
2.8. Applies communications security programs to include physical, cryptographic, transmission, and emission security. Develops and ensures compliance with safety standards and instructions.
2.9. As a 3D1X2R performs, coordinates, integrates and supervises network design, configuration, operation, defense, restoration, and improvements on radio frequency wireless, line-of-sight, beyond line-of-sight, wideband, and ground-based satellite and encryption transmission devices in a fixed and deployed environment. Analyzes capabilities and performance, identifies problems, and takes corrective action. Deploys, sustains, troubleshoots and repairs standard radio frequency mission-specific systems and devices. Establishes and maintains circuits, configures and manages system and network connectivity.
2.10. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]
2.11. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge of electronic and network principles, information assurance, telephony, copper and fiber-optic transmission principles, cryptographic techniques, network system installation practices, project and circuit diagram interpretation, test equipment, special tools, and management practices is mandatory.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in mathematics, computer science, computer principles or information technologies is desirable. Any computing or network commercial certification is desirable.

3.3. Training. For award of AFSC 3D132, completion of Cyber Transport initial skills course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D152. Qualification in and possession of AFSC 3D132. Also, experience in installation, maintenance, and repair of voice, data and video network infrastructure and cryptographic equipment.

3.4.2. 3D172. Qualification in and possession of AFSC 3D152. Also, experience in supervising installation, maintenance, and repair of voice, data and video network infrastructure and cryptographic equipment.

3.5. Other: The following are mandatory as indicated:

3.5.1. For entry into this specialty:

3.5.1.1. Normal color vision as defined in AFI 48-123, *Medical Examinations and Standards*.

3.5.1.2. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Vehicle Operations* is desired.

3.5.1.3. See Attachment 4 for additional entry requirements.

3.5.2. For award and retention of this AFSC:

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.2.2. Specialty routinely requires work in the networking environment.

3.5.2.3. Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program* and to DoD 8570.01-M, *Information Assurance Workforce Improvement Program*.

3.5.2.4. Specialty requires routine access to Tier 5 (T5) information, systems or similar classified environments.

3.5.3. For award and retention of AFSCs 3D152/72:

3.5.3.1. Completion of a current T5 background investigation according to AFMAN 16-1405, *Personnel Security Program Management* is mandatory.

3.5.3.2. Must maintain a T5 clearance for retention of this AFSC.

NOTE: Award of entry level without a completed T5 Investigation is authorized provided an interim Top Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D173, Craftsman
AFSC 3D153, Journeyman
AFSC 3D133, Apprentice
AFSC 3D113, Helper

<div align="center">

★**RF TRANSMISSION SYSTEMS**
(Changed 31 Oct 20)

</div>

1. Specialty Summary. Deploys, sustains, troubleshoots and repairs standard radio frequency wireless, line-of-sight, beyond line-of-sight, wideband, and ground-based satellite and encryption transmission devices in a fixed and deployed environment. Included are multiple waveform systems operating across the spectrum, keying and signal devices; telemetry, and instrumentation systems. Establishes and maintains circuits, configures and manages system and network connectivity. Manages organizational LMR device accounts. Related DoD Occupational Subgroup: 110100.

2. ★Duties and Responsibilities:

2.1. Performs/supervises wireless radio and satellite systems and equipment maintenance activities. Oversees work in progress and reviews completed repairs for sound maintenance practices. Establishes requirements for maintenance equipment, support equipment, tools, and spare parts. Requisitions, accounts for, and turns in supplies and material. Interprets inspection findings and determines adequacy of corrective action. Reviews and ensures compliance with maintenance management publications and procedures. Identifies maintenance problem areas and recommends corrective action. Recommends methods to improve equipment performance and maintenance procedures. Evaluates justification and practicability of proposed modifications. Develops and enforces safety standards for ground RF system maintenance activities.

2.2. Inspects wireless radio/satellite communications activities. Determines equipment operational status. Serves on teams to evaluate transmission systems activities. Interprets inspection findings submitted by other inspecting activities, and initiates corrective action. Determines adequacy of corrective action. Checks installed and repaired components for compliance with technical publications.

2.3. Resolves installation, repair, overhaul, and modification problems associated with communications equipment. Employs orbiting communication satellite, line-of-sight, and tropospheric scatter techniques. Installs, maintains, reconstitutes, removes, and modifies coaxial cabling, waveguide and antenna systems. Conducts tests to restore and maintain systems. Uses anti-jam equipment and techniques to neutralize effects of communication jamming. Uses layout drawings, schematics, and pictorial diagrams to solve maintenance problems. Analyzes construction and operating characteristics of equipment to determine source of malfunction. Performs intricate alignment and calibration procedures to ensure maximum operating efficiency. Determines repair procedures necessary to correct defective equipment.

2.4. Installs ground radio, satellite, and telemetry communications equipment. Consults layout drawings to ensure equipment is properly positioned. Checks equipment for serviceability prior to installation. Assembles, connects, secures, and interconnects components such as transmitters, power supplies, and antenna assemblies. Tests installed equipment for proper assembly of components and compliance with technical orders. Places in operation and tunes, adjusts, and aligns components to obtain maximum operating efficiency. Identifies and locates Radio Frequency interference sources.

2.5. Deploys and activates mobile and transportable transmission equipment. Refers to plans and equipment specifications to conduct site and equipment surveys, and establishes equipment systems interface. Unpacks, inspects, and positions communications equipment; erects antennas; and interconnects communications facilities.

2.6. Performs preventive maintenance on communications systems and related equipment. Inspects equipment at specified intervals to determine operational status. Replaces defective components. Performs operational checks. Updates maintenance data collection records and systems to document actions completed.

2.7. Repairs, overhauls, and modifies communications and related equipment. Isolates malfunctions using system checking procedures, required test equipment, analyzing voltage and waveform measurements, schematic diagrams, and equipment operating characteristics. Repairs equipment, including transmitters, receivers, transceivers, and related equipment. Tunes and adjusts components. Adjusts, aligns, and calibrates equipment for maximum operating efficiency. Fabricates and connects various types of antenna systems and transmission lines. Understands antenna fundamentals, including antenna theory and principles of rotators, amplifiers and control cables. Tests repaired components using bench mockups and related test equipment.

2.8. Maintains inspection and maintenance records to include organizational device accounts. Posts entries on maintenance and inspection records. Records meter readings and other pertinent data in equipment logs. Completes maintenance data collection forms.

2.9. ★Performs installation spectrum management duties during temporary absence of qualified Spectrum Operations (3D1X4) personnel. Engineers, nominates, assigns, and proactively ensures access to frequencies that support communications and operational requirements. Coordinates frequency needs with Federal, military, and civil spectrum management agencies. Secures operating authority, and ensures the least possible interference is caused or received by Air Force electromagnetic systems. Drafts and reviews spectrum interference reports. Resolves electromagnetic interference problems with the use of spectrum analysis software, and spectrum scanning equipment.

2.10. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings

<div align="center">

209

</div>

for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]

2.11. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge of: electricity and radio theory, including transistors, solid-state components, and digital techniques applying to ground RF communications and related equipment maintenance; and interpretation of management information data, technical orders, blueprints, wiring diagrams, and schematic drawings is mandatory.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in physics and mathematics is desirable. Any computing or network commercial certification is desirable.

3.3. Training. For award of AFSC 3D133, completion of RF Transmissions Systems initial skills course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D153. Qualification in and possession of AFSC 3D133. Also, experience in functions such as; testing, tuning, adjusting, maintaining, or repairing ground RF communications and related equipment, and using specialized test equipment.

3.4.2. 3D173. Qualification in and possession of AFSC 3D153. Also, experience supervising functions such as siting, installing, repairing, overhauling, or modifying ground RF equipment, and using test equipment.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty:

3.5.1.1. Normal color vision as defined in AFI 48-123, *Medical Examinations and Standards*.

3.5.1.2. See attachment 4 for additional entry requirements.

3.5.2. For award and retention of this AFSC:

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.2.2. Specialty requires routine access to Tier 3 (T3) information, systems or similar classified environments.

3.5.3. For award and retention of AFSCs 3D153/73:

3.5.3.1. Completion of a current T3 background investigation according to AFMAN 16-1405, *Personnel Security Program Management.*

NOTE: Award of the entry level without a completed T3 Investigation is authorized provided an interim Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D174, Craftsman
AFSC 3D154, Journeyman
AFSC 3D134, Apprentice
AFSC 3D114, Helper

★**SPECTRUM OPERATIONS**
(Changed 31 Oct 20)

1. Specialty Summary. The Spectrum Operations technician analyzes requirements and requests frequencies to support terrestrial, aircraft, and space systems and coordinate radio, radar, land, and other electromagnetic radiating or receiving requirements. They possess a solid understanding of wireless communications systems technologies and Electronic Warfare (EW) tactics, techniques, and procedures, and serves as counsel to commanders and combatant commanders on all spectrum issues. They also provide guidance to program offices, developers, and potential users of spectrum dependent equipment planned for purchase or modification before being introduced into the Air Force inventory. Related DoD Occupational Subgroup: 120100.

2. Duties and Responsibilities:

2.1. Engineers, nominates, assigns, and proactively ensures access to frequencies that support communications and operational requirements. Coordinates frequency needs with Federal, military, and civil spectrum management agencies. Secures operating authority, and ensures the least possible interference is caused or received by Air Force electromagnetic systems. Drafts and reviews spectrum interference reports. Resolves electromagnetic interference problems with the use of spectrum analysis software, and spectrum scanning equipment.

2.2. Determines risk assessment and provides sound advice to commanders and combatant commanders on mission impacts and collateral damage.

2.3. Collaborates with signals intelligence specialists in the identification, monitoring, and exploitation of emissions, in order to better control the electromagnetic battlespace.

2.4. Analyzes radio frequency spectrum requirements and determines compatibility with other users considering transmitter and receiver specifications, antenna data, emission characteristics, and modes of radio wave propagation. Examines radio link deficiencies and recommends corrective action to improve system performance. Recommends solutions to electromagnetic compatibility problems.

2.5. Manages and updates frequency records in a classified database shared by the joint spectrum community in order to provide a global understanding of the spectrum environment. Provides guidance on the spectrum certification process for electromagnetic spectrum dependent equipment planned for introduction into the Air Force inventory, and for modifications to existing equipment. Reviews planning and program documents to determine whether spectrum support is required. Prepares frequency annexes for contingency and operations plans. Examines spectrum allocation data and frequency assignment records to ascertain suitability of specific equipment planned for deployment.

2.6. Performs as joint task force spectrum manager. Provides spectrum management guidance to units deploying radio frequency equipment to support contingency, exercise, or wartime requirements. Analyzes and de-conflicts frequency assignments and databases to develop joint communications and electronics operating instructions.

2.7. Evaluates and assists electromagnetic spectrum management activities. Determines if spectrum support is adequate and recommends changes. Educates customers on optimal and proper use of the electromagnetic spectrum. Plans for current and future electromagnetic spectrum needs. Identifies and locates Radio Frequency interference sources using spectrum analysis software, and spectrum scanning equipment.

2.8. Conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. Specialty Qualifications:

3.1. Knowledge. Knowledge is mandatory of:

3.1.1 Radio propagation factors, including effects of antenna design, power, emission type, frequency, and effects of terrain.

3.1.2 National, international, and military regulations governing use of the electromagnetic spectrum.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in algebra, geometry, and physics is desirable. (Does not require HS diploma for retrainees coming from Para 3.5.1.3.)

3.3. Training. The following training is mandatory for award of the AFSC indicated:

3.3.1 For award of AFSC 3D134, completion of Spectrum Operations initial skills course is mandatory.

3.4 Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. 3D154. Qualification in and possession of AFSC 3D134. Also, experience performing spectrum management engineering, selection, negotiation, and resolution of interference problems.

3.4.2. 3D174. Qualification in and possession of AFSC 3D154. Also, increased experience performing and/or supervising personnel in problem solving, electromagnetic spectrum management, engineering, selection and negotiation techniques, and resolution of

interference problems. Possesses a good understanding of offensive spectrum operating environments and is able to advise commanders/stakeholders on risk issues during these offensive activities.

3.5. Other. The following are mandatory as indicated.

3.5.1. For entry into this specialty:

3.5.1.1. See attachment 4 for additional entry requirements.

3.5.1.2. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Ground Transportation* is desired.

3.5.1.3. Prior qualification in AFSCs 1A3X1, 1C4X1, 1C5X1, 1C6X1, 1C8XX, 1N2X1, 1N4X1, 2A0X1P, 2A2X3A, 2A5X3, 2A8X1, 2A9X3B or 3D1XX at the 5-skill level or higher (3-skill level if no 5-skill level exists).

3.5.1.4. Other AFSCs not listed in paragraph 3.5.1.3 will be considered as a retraining exception to policy (ETP) with Career Field Manager (CFM) approval.

3.5.2. For award and retention of this AFSC,

3.5.2.1. Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*

3.5.2.2. Specialty requires routine access to Tier 5 (T5) information, systems or similar classified environments.

3.5.3. For award and retention of AFSC 3D154/74:

3.5.3.1. Completion of a current T5 background investigation according to AFMAN 16-1405, *Personnel Security Program Management* is mandatory.

3.5.3.2. Must maintain a T5 Investigation for retention of this AFSC.

3.5.2.5. When required for a current or future assignment, must successfully complete and pass a Counterintelligence (CI) polygraph test.

NOTE: Award of entry level without a completed T5 Investigation is authorized provided an interim Top Secret security clearance has been granted according to AFMAN 16-1405.

AFSC 3D177, Craftsman
AFSC 3D157, Journeyman
AFSC 3D137, Apprentice
AFSC 3D117, Helper

★**CABLE AND ANTENNA SYSTEMS**
(Changed 31 Oct 20)

1. **Specialty Summary.** Provides command and control (C2) capabilities through installation, maintenance, fault isolation, and reconstitution of fixed cable and wireless distribution systems, local area networks (LAN), and wide area networks (WAN) in support of tactical and strategic operations. Monitors and analyzes performance of underground, buried, and aerial cable and antenna networks. Related DoD Occupational Subgroup: 162100.

2. **Duties and Responsibilities**:
2.1. Installs, maintains, reconstitutes, removes, and modifies copper core, coaxial, waveguide, and fiber optic cable and antenna systems. Climbs antenna support structures and wooden poles to various heights for maintenance and installation actions on cable and antenna systems. Installs and maintains dedicated local area network (LAN) and wide area network (WAN) media distribution systems, including distribution system interior wiring. Installs and removes fire stopping barriers when installing interior cabling. Uses drawings, task lists, instructions, and technical data to work on copper core, coaxial, waveguide, fiber optic cable and antenna systems. Installs distribution equipment. Terminates copper core, coaxial, waveguide, and fiber optic cable on distribution frames and interface equipment. Operates and performs maintenance using tools, test equipment, auxiliary equipment, and vehicles such as backhoes, trenchers, cable trailers, cable reel trucks, and antenna construction vehicles.
2.2. Locates, repairs, and replaces faulty closures in copper core, waveguide, coaxial, and fiber optic cable systems. Performs pneumatic troubleshooting to locate faulty splice closures and seals splice closures. Excavates and backfills splice pits. Installs and maintains aerial cable support structures such as pole line and suspension strands. Installs underground cable, uses duct rods, cleans cable duct systems, prepares pulling apparatus, and pulls in and temporarily bonds cable. Installs, maintains, and marks path of buried cable systems.
2.3. Monitors, analyzes, and troubleshoots copper core, waveguide, coaxial, and fiber optic cable systems. Determines cause of signal deterioration in cable carrying audio, video, digital, and data transmission. Interprets compressor meter readings and adjusts controls. Installs, maintains, and repairs or replaces damaged pneumatic components in cable air dryers. Uses test equipment to identify copper conductors and optic fibers in cables. Locates and traces buried cable. Locates and traces leaks in pressurized cable system. Performs operational checks and preventive maintenance inspections.
2.4. Maintains communications and computer systems installation records, maintenance and inspection cable records, and technical orders.
2.5. Supervises, plans, organizes, and directs cable and antenna installation and maintenance activities. Develops and improves work methods and procedures related to installation and maintenance of all cable and antenna systems.
2.6. As part of the Cyberspace Support career field family, performs IT project management duties to include; manage, supervise, and perform planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as advisor at meetings for facility design, military construction programs and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems. [DCWF Code - 802]
2.7. As part of the Cyberspace Support career field family, conducts defensive cyber operations (DCO) and associated support activities to defend DoD and other friendly cyberspace. DCO includes passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems as well as passive defense measures intended to maintain and operate the DODIN and other networks such as configuration control, patching and firewall operations. Support activities includes but not limited to maintenance of cyber weapons systems, functional mission analysis, mission mapping, tool development, stan-eval, mission planning and data analysis. [DCWF Code - 511, 521, 531, 541]

3. **Specialty Qualifications:**
3.1. Knowledge. Knowledge of the following is mandatory: installation and maintenance management functions; wire transmission principles; electrical and light wave communications on aerial, buried and underground cable systems; cable pressure and alarm systems; antenna and obstruction systems; antenna fundamentals, including antenna theory and principles of rotators, amplifiers and control cables; antenna installation procedures, including radio frequency cable, waveguide splicing, and repair and maintenance techniques of radomes; operation and theory of cable pressurization, alarm systems, locating cable faults, identifying causes of deterioration in cable systems, cable testing procedures and methods of sealing cables; safety precautions related to oxygen deficiency, oxygen enrichment, toxic and explosive gases, working aloft, rescue procedures for aerial and underground environments, basic first

aid and cardiopulmonary resuscitation; use and limitations of test set operations; corrosion prevention and control procedures; and capabilities, limitations, operations and functional use of basic cable and antenna systems and associated hardware is mandatory.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in mathematics, computer science or information technologies are desirable.

3.3. Training. For award of AFSC 3D137, completion of Cable and Antenna Systems initial skills course is mandatory.

3.4. Experience. The following experience is mandatory for the award of the AFSC indicated:

3.4.1. 3D157. Qualification in and possession of AFSC 3D137. Also, experience in functions such as installing, maintaining and repairing communications cable and antenna systems, including electrical equipment and transmission lines.

3.4.2. 3D177. Qualification in and possession of AFSC 3D157. Also, experience performing or supervising functions in areas such as project installation and maintenance actions, communications cables and antennas, and related electrical hardware.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty:

3.5.1.1. Normal color vision as defined in AFI 48-123, *Medical Examinations and Standards*.

3.5.1.2. A valid state driver's license to operate government motor vehicles (GMV) in accordance with AFI 24-301, *Vehicle Operations* is desired.

3.5.1.3. See attachment 4 for additional entry requirements.

3.5.2. For entry, award and retention of these AFSCs:

3.5.2.1. Normal depth perception and normal gait and balance as defined in AFI 48-123.

3.5.2.2. Physical ability to perform climbing duties and freedom from fear of heights and claustrophobia.

3.5.3. For award and retention of this AFSC:

Must maintain local network access IAW AFI 17-130, *Cybersecurity Program Management* and AFMAN 17-1301, *Computer Security.*