Military Branch: Air Force

Military Occupation: CYBERSPACE DEFENSE OPERATIONS
Military Code: AFSC 1B4X1

Training Levels: All Air Force occupations have up to 5 different training levels: Helper, Apprentice, Journeyman, Craftsman and Superintendent.

Below are training levels with Occupation codes:

AFSC 1B471, Craftsman	**AFSC 1B431, Apprentice**
AFSC 1B451, Journeyman	**AFSC 1B411, Helper**

Go To: Occupation Details Civilian Competencies

(Changed 31 Oct 13, Effective 28 Feb 13)
1. Specialty Summary. Performs duties to develop, sustain, and enhance network capabilities to defend national interests from attack and to create effects in cyberspace to achieve national objectives. They enable net-centric command and control (C2) systems to synchronize cross-domain attack operations and de-conflict friendly use of cyberspace. They conduct network attack, network defense, and network exploitation operations using on-net tools, tactics, techniques and procedures to achieve COCOM and national objectives**.** They will partner with Joint and coalition services to detect, deny, disrupt, deceive, and mitigate adversarial access to sovereign national networks and systems. The duties performed by Cyberspace Defense Operators include: operating cyberspace warfare systems; performing technical analysis of networks and systems in support of national level objectives. Related DoD Occupational Subgroup: None.

2. Duties and Responsibilities:
2.1. Directs personnel and cyberspace warfare operations. Selects and employs surveillance, combat, reporting and network management systems. Interprets directives into specific guidance and procedures for operator actions. Develops and executes operations plans to ensure positive control of assigned resources. Evaluates operational readiness of communications, sensors, intrusion detection, and related support equipment. Coordinates with other operators performing weapons control, surveillance, and network activities. Advises commander on readiness of capabilities, status reports, training exercises, and evaluation results.

2.2. Develops and executes tactics, techniques, and procedures (TTP) in support of cyberspace full spectrum operations. Analyzes national defense guidance and objectives to create operational policies. Implements policy through development of TTPs to execute assigned weapons and C2 capabilities.

BELLEVUE COLLEGE

This workforce solution was 100% funded by an $11.7m grant awarded by the U.S. Department of Labor's Employment and Training Administration, Grant #TC-23745-12-60-A-53. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Plans, conducts, and evaluates exercises to enhance operational readiness. Ensures interoperability of assigned weapons systems with joint/coalition partners. Establishes procedures and monitors implementation of programs, policies, and plans. Implements operational TTPs with DoD, allied forces, and civil authorities.

2.3. Establishes performance standards, trains and conducts evaluations to ensure personnel are proficient, qualified, and certified. Ensures units meet operational readiness goals and adhere to operational procedures. Coordinates with other agencies to ensure resources are adequate to accomplish missions.

2.4**.** Participates in research, development and operational testing and evaluation to determine new capabilities and modifications to existing systems. Assesses and reverse engineers network nodes and infrastructure devices; to include operating systems and software applications to determine capabilities, functionalities, limitations and vulnerabilities. Assists in writing technical requirements, analyzing equipment specifications, and developing criteria to ensure operational effectiveness.

2.5. Performs network attack activities to include effects gained from emerging technology such as: disruption, data manipulation, degradation, destruction and denial of C2 while maintaining operational situational awareness. Network warfare operations include activities on an adversary's communication infrastructure and equipment.

2.6. Conducts network defense operations of friendly forces and vital interests from hostile attacks. Defense techniques consist of active and passive cyberspace operations including employment of defensive measures designed to deny attacking adversaries or reduce their effectiveness. Network defense includes measures to preserve, protect, recover, and reconstitute friendly cyberspace capabilities before, during, and after a hostile attack. Network defense encompasses cyberspace attack deterrence, attack mitigation and survivability, attack attribution, vulnerability detection and response, data protection, and infrastructure protection.

2.7. Provides command and control of network warfare operations with DoD, interagency and Coalition Forces to establish situational awareness of both friendly and adversary operations.

2.8. When directed, act with federal, state, and local governments, as well as private sector parties, to identify dependencies and reduce vulnerabilities before they can be exploited. Defends and secures national critical infrastructure and national interests.

BELLEVUE COLLEGE

This workforce solution was 100% funded by an $11.7m grant awarded by the U.S. Department of Labor's Employment and Training Administration, Grant #TC-23745-12-60-A-53. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

2.9. Performs battle damage assessments and analysis on network hardware and software components. Applies forensic and reverse engineering TTPs to determine the extent of the battle damage sustained during cyber attacks. AFECD, 31 October 2013 42

3. Specialty Qualifications:
3.1. Knowledge. Knowledge is mandatory of: computer operating systems, software applications, protocols, addressing and hardware. Also mandatory, understanding networking fundamentals, network infrastructure, telecommunications theory and data communications. They must be proficient on wireless networking as well as delivery to personal wireless devices and understand cryptography, to include utilization and exploitation techniques.
3.2. Education. For entry into this specialty, completion of high school is mandatory. Additional courses in physics, computer science and mathematics is desirable. Associate degree or higher in related fields or Information Technology (IT) certification is desirable.
3.3. Training. For award of AFSC 1B431, completion of Cyberspace Defense Operations initial skills course is mandatory.
3.4. Experience. The following experience is mandatory for award of the AFSC indicated:
3.4.1. 1B451. Qualification in and possession of AFSC 1B431. Also, experience performing functions such as network attack, defense, and exploitation.
3.4.2. 1B471. Qualification in and possession of AFSC 1B451. Also, experience performing and supervising functions such as network attack, defense, and exploitation.
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. Prior qualification at the 5-skill level or higher in any AFSC (desirable AFSCs: 3D0X2, 3D0X3, 3D0X4, 3D1X1, 3D1X2, 1N2X1, or 1N4X1).
3.5.1.3. Normal color vision according to AFI 48-123, *Medical Examinations and Standards.*
3.5.2. For award and retention of these AFSCs, must maintain an Air Force Network License according to AFI 33-115, Vol 2, *Licensing Network Users and Certifying Network Professionals.*
3.5.3. Specialty routinely requires work in the networking environment. For award and retention of AFSCs 1B431/1B451/1B471, must attain and maintain a minimum Information Assurance Technical Level II certification according to DoD 8570.01-M, *Information Assurance Workforce Improvement Program*.
3.5.4. Specialty requires routine access to Top Secret material or similar environment. For award and retention, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, *Personnel Security Program Management,* is mandatory.

NOTE: Award of the 3-skill level without a completed SSBI is authorized provided an interim Top Secret clearance has been granted according to AFI 31-501.

BELLEVUE COLLEGE

This workforce solution was 100% funded by an $11.7m grant awarded by the U.S. Department of Labor's Employment and Training Administration, Grant #TC-23745-12-60-A-53. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Materials included in these reports are from:

• The AIR FORCE ENLISTED CLASSIFICATION DIRECTORY (AFECD)-The Official Guide to the Air Force Enlisted Classification Codes- Published October 2013

• The Department of Labor's My Next Move pages and links.

• The USAF public web pages.

BELLEVUE COLLEGE

This workforce solution was 100% funded by an $11.7m grant awarded by the U.S. Department of Labor's Employment and Training Administration, Grant #TC-23745-12-60-A-53. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.