Military Branch: Air Force

Military Occupation: CYBER SURETY

Military Code: AFSC 3D0X3

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

Go To: **Occupation Details** **Civilian Competencies**

(Changed 31 Oct 13, Effective 28 Feb 13)

1. Specialty Summary. Supervises or operates fixed and deployed 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. Identifies potential threats and manages resolution of security violations. Enforces national, DoD and Air Force security policies and directives; employs hardware and software tools to enhance the security by installing, monitoring and directing proactive and reactive information protection and defensive measures to ensure Confidentiality, Integrity and Availability (CIA) of IT resources. Administers and manages the overall Information Assurance (IA) 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 IA risk and vulnerability assessments; ensures enterprise IA policies fully support all legal and regulatory requirements and ensures IA policies are applied in new and existing IT resources. Identifies IA weaknesses and provides recommendations for improvement. Monitors enterprise IA policy compliance and provides recommendations for effective implementation of IT security controls.

2.2. Evaluates and assists IT activities. Makes periodic evaluation and assistance visits, notes discrepancies, and recommends corrective actions. Audits and enforces the compliance of IA procedures and investigates security-related incidents. Assists in conducting IT forensic investigations. Manages the IA program and monitors emerging security technologies and industry best practices.

□2.3. Performs or supervises detection and protection activities using IA and IA-enabled tools. Responsible for IA oversight or management of national security systems during all phases of the IT life cycles. Ensures CIA of IT resources.

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.

□2.4. Operates and manages IA tools and IA-enabled tools. Integrates tools with other IT functions to protect and defend IT resources. Provides CIA by verifying IA controls are implemented in accordance with DoD and Air Force IA standards. Ensures appropriate administrative, physical, and technical safeguards are incorporated into all new IT resources through certification and accreditation and protects IT resources from malicious activity.

2.5. Installs, upgrades, configures and maintains IA tools and IA-enabled tools; develops scripts and macros to automate tedious tasks and ensure data survivability through IA controls.

□2.6. Performs COMSEC management duties in accordance with national and DoD directives. Maintains primary site account for all required physical and electronic COMSEC material. Issues all material to subordinate units and provides guidance and training to unit level COMSEC Responsible Officers. Conducts inspections to ensure COMSEC material is properly maintained and investigates and reports all COMSEC related incidents.

□2.7. Performs EMSEC or TEMPEST as it is otherwise known, duties in accordance with national and DoD TEMPEST standards. Denies unauthorized access to classified, and in some instances, unclassified information via compromising emanations within an inspectable space through effective countermeasure application. Ensures all systems and devices comply with national and DoD TEMPEST 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.

□2.8. Combat Crew Communications (CCC) technicians train and equip airlift, bomber, early warning, reconnaissance, and tanker aircrews. CCC's areas of responsibility include but are not limited to Communications Security, Flight Information Publications, Identification, Friend or Foe/Selective Identification Feature, Combat Mission Folders, High Frequency, Milstar, Very Low Frequency/Low Frequency, aircrew training, and programming communications equipment. Support prepares aircrews to execute global conventional and strategic (nuclear) taskings from combatant commanders, Joint Chiefs of Staff (JCS), and the US Strategic Command (USSTRATCOM).

2.9. Manages, supervises, and performs 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 status of 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.AFECD, 31 October 2013 193

3. Specialty Qualifications:

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.

3.1. Knowledge. Knowledge is mandatory of: IT resources; capabilities, functions and technical methods for IT operations; organization and functions of networked IT resources; communications-computer flows, operations and logic of electromechanical and electronics IT and their components, techniques for solving IT operations problems; and IT resources security procedures and programs including Internet Protocol and basic software scripting.

□3.2. Education. For entry into this specialty, completion of high school is mandatory. Additional courses in advanced mathematics, computer science and networking is desirable. Experience in systems administration in an UNIX, Linux/MacOS, or Windows environment and/or software development, testing, and quality assurance is desired. Network+ certification or equivalent 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 IA functions and/or activities.

3.4.2. 3D073. Qualification and possession of AFSC 3D053. Experience supervising IA functions and/or activities.

3.5. Other. The following are mandatory as indicated:

3.5.1. See attachment 4 for additional entry requirements.

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 3D033/3D053/3D073, must attain and maintain a minimum Information Assurance Management Level I 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 of AFSCs 3D033/53/73, 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 security clearance has been granted according to AFI 31-501.

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.**

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.