BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1303

12 MAY 2020

Cyberspace Operations

AIR FORCE CYBERSECURITY WORKFORCE IMPROVEMENT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at **www.e-publishing.af.mil** for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNSF

Certified by: SAF/CNS
(Maj Gen Kevin Kennedy)

Supersedes: AFMAN17-1303, 20 March 2015

Pages: 85

This publication implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*. It provides guidance and procedures on AF cybersecurity workforce positions, training, certifications, qualifications requirements and policy on cyber workforce reporting, metrics and validation throughout the Air Force (AF). This manual applies to all civilian employees and uniformed members of the Regular Air Force, Air National Guard and Air Force Reserve, as well as to Air Force contractors when required by the terms of their contracts. Direct questions, comments, recommended changes, or conflicts to this publication through command channels using the AF Form 847, *Recommendation for Change of Publication*, to SAF/CN. Send any supplements to this publication to SAF/CN for review, coordination, and approval prior to publication. The authorities to waive wing or unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program,* and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This publication has been revised. Major changes include updates to the certification DoD approved cybersecurity baseline certification requirements for specific roles (e.g., Authorizing Official Designated Representative [AODR]); stipulates minimum certification requirements for various cyber roles and risk management positions; mandates certification requirement for those civilian, military, or contractors performing in senior software developer, senior software subject expert or senior software tester role(s); revises the special experience identifier (SEI) lists for civilians and military (officer and enlisted); codifies the computing environment or operating system training completion certificate requirement, including acceptable documentation; revamps the certification determination guide (**Attachment 2**) by category or specialty and level.

Chapter 1—GENERAL INFORMATION 5

1.1. Introduction. 5

1.2. General Guidance. 5

1.3. Requirements. 5

Chapter 2—ROLES AND RESPONSIBILITIES 7

2.1. Air Force Deputy Chief Information Officer (SAF/CN). 7

2.2. Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance and Cyber Effects Operations (AF/A2/6) 8

2.3. Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services (AF/A1). 8

2.4. Assistant Secretary of the Air Force, Acquisition, Technology & Logistics (SAF/AQ). 8

2.5. Director of Security, Special Programs Oversight (SAF/AAZ). 9

2.6. Air Force Career Field Manager(s). 9

2.7. MAJCOMs. 9

2.8. Air Combat Command. 9

2.9. Air Education and Training Command. 10

2.10. Air Force Personnel Operations Agency. 10

2.11. Air Force Personnel Center. 10

2.12. Authorizing Officials. 10

2.13. Wing Cybersecurity Office (WCO). 10

2.14. Program or Project Managers (PMs), System Managers, Program Management Offices (PMOs), Developmental or Operational Test Agencies, and Units. 11

2.15. Contracting Officer. 13

2.16. Information System Security Managers (ISSMs). 14

2.17. Civilian Personnel Section. 14

2.18. Supervisors. 14

2.19. Individuals (Civilian and Military). 14

2.20. Individuals (Contractor Personnel). 15

Chapter 3—CYBERSECURITY WORKFORCE IDENTIFICATION 16

3.1. Position Identification. 16

3.2. Cybersecurity Workforce. 16

3.3. Primary, Additional, and Embedded Duty. 24

3.4. Recording the Cybersecurity Workforce Position Requirement. 24

Table 3.1. Civilian SEIs (Positions Coded with Equivalent Enlisted Air Force Specialty Codes). 25

Table 3.2. Civilian SEIs (Positions Coded with Equivalent Officer AFSCs). 26

Table 3.3. Enlisted SEIs. 28

Table 3.4. Officer SEIs. 29

3.5. Deployments and Unit Type Code (UTC). 30

Chapter 4—WORKFORCE QUALIFICATIONS 31

4.1. Qualified Cybersecurity Workforce Criteria. 31

4.2. Computing Environment or Operating System Training Completion Requirement. 31

4.3. Privileged User Agreement 32

4.4. Additional Cybersecurity Certification Requirement. 32

Chapter 5—CYBERSECURITY WORKFORCE CERTIFICATION PROCESS 33

5.1. Cybersecurity Baseline Certifications. 33

5.2. Air Force Preferred Cybersecurity Baseline Certifications (Civilian and Military Only). 33

5.3. Minimum Cybersecurity Baseline Certification Requirement. 33

5.4. Support for the Cyber Operations Career Field (17XX). 34

5.5. Exams (Civilians and Military Only). 34

5.6. Certification Exam Failure or Decertification. 34

5.7. Continuing Education Units (CEUs) or Continuing Professional Education (CPE). 36

5.8. Maintenance of Cybersecurity Baseline Certifications... 37

5.9. Recording Certification Completion. 37

5.10. Recording Computing Environment or Operating System Training Completion. .. 38

5.11. Community College of the Air Force Credit. 38

Chapter 6—CYBERSECURITY WORKFORCE TRAINING 39

6.1. Initial Skills Training.. 39

6.2. Training Resources. 39

6.3. Authorizing Official Training. 39

6.4. Contracted Training. 39

6.5. Military Computing Environment or Operating System Training Options. 39

6.6. Civilian Computing Environment or Operating System Training Options. 39

6.7. Contractor Computing Environment or Operating System Training Options. 40

Chapter 7—CYBERSECURITY BASELINE CERTIFICATION WAIVERS (CIVILIANS AND MILTARY ONLY) 41

7.1. In accordance with DoD 8570. 41

7.2. Waiver Process. 41

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 42

Attachment 2—Air Force Cybersecurity Workforce Position Certification Determination Guide – Technical Category Matrix 46

Attachment 3—Military Certification Failure Policy 77

Attachment 4—CYBERSECURITY WORKFORCE METRIC REPORT 80

Attachment 5—FORMAL STATEMENT OF RESPONSIBILITES (APPLICABLE FOR CIVILIANS AND MILITARY) 82

Attachment 6—FORMAL STATEMENT OF RESPONSIBILITIES (APPLICABLE FOR CONTRACTORS) 85

Chapter 1

GENERAL INFORMATION

1.1. Introduction.

1.1.1. In accordance with DoD Directive (DoDD) 8140.01, *Cyberspace Workforce Management* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, the goal of the AF Cybersecurity Workforce Improvement Program is to "develop a DoD cybersecurity workforce with a common understanding of the concepts, principles, and applications of cybersecurity for each category, level, and function to ensure the confidentiality, integrity, and availability of DoD information, Information Systems, networks, and information stored within." The AF Cybersecurity Workforce Improvement Program provides warfighters qualified cybersecurity personnel in the following roles to develop, use, operate, administer, maintain, defend, dispose of, and retire DoD Information Systems: Authorizing Officials, Information Assurance Technical (IAT), Information Assurance Management (IAM), Cyber Security Service Providers (CSSP) (formerly called Computer Network Defense-Service Provider), and Information Assurance System Architects and Engineers (IASAEs). This manual identifies AF cybersecurity workforce positions, certification and qualifications requirements, and provides policy on cybersecurity workforce reporting, metrics, and validation. Cybersecurity workforce personnel are classified by tasks and associated DoD approved baseline cybersecurity certifications category (IAT and IAM) or specialty (CSSP and IASAE). Unless noted, the cybersecurity requirements (e.g., certification, training, etc.) specified in this manual are the minimum required. Commanders are authorized to increase requirements to reflect specific missions.

1.2. General Guidance.

1.2.1. AFMAN 17-1303 compliance is required for the AF Intelligence Community and Special Access Program unless this AFMAN conflicts with the Office of Director of National Intelligence or the DoD Director, Special Access Programs Central Office, DoD Directive 5205.07, *Special Access Program (SAP) Policy*. When in conflict, the Office of Director of National Intelligence and DoD Special Access Programs Central Office guidance take precedence for the AF Intelligence and Special Access Program Communities.

1.2.2. DoD 8570.01-M requirements have been vetted through Office of the Secretary of Defense legal channels and with National Unions. That said, the DoD Chief Information Officer (DoD CIO) has strongly recommended continuous engagements with appropriate local parties (e.g., the Human Resources section of the Office of Personnel Management or local unions).

1.2.3. This manual does not address the operational employment of the cybersecurity roles. Operational employment of the cybersecurity workforce are determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.

1.3. Requirements.

1.3.1. All users who need access to the AF Information Networks (AFIN), Information System, or Platform Information Technology (PIT) System will complete initial cybersecurity user awareness training as a condition of access in accordance with DoD 8570.01-M, Paragraph C6.2.2. **(T-0)**

1.3.1.1. All users will complete the annual cybersecurity user awareness refresher training to maintain network or system access. **(T-1)**

1.3.1.2. All users will accomplish the required cybersecurity user awareness training via SAF/CN approved methods. **(T-1).** The list of approved training methods includes, but is not limited to, the following: (1) using the AF learning management system (e.g., Advanced Distributed Learning Service, AF Learning Services Ecosystem); (2) using the DoD Cyber Exchange NIPR (Nonclassified or Nonsecure Internet Protocol Router) portal: **https://cyber.mil/**; or (3) using any other method that SAF/CN designates. Using the AF learning management system is the preferred training method.

1.3.2. All AF civilian and military cybersecurity workforce positions performing at least one cybersecurity task will be identified on a Unit Manning Document (UMD) using established SEIs. **(T-1)**

1.3.3. For civilian and military personnel, the cybersecurity workforce information will be recorded in manpower and personnel databases or systems (e.g., Military Personnel Data System and Defense Civilian Personnel Data System [DCPDS]), to include but not limited to, AF Specialty Code (AFSC) or civilian occupational series. **(T-0)**

1.3.4. For contractors, all cybersecurity requirements, including currency, must be listed in the contract requirements and associated statement of work or performance work statement DoD 8570.01-M, Paragraph C1.4.4.5. **(T-0).** Details on the contractor cybersecurity workforce must be locally collected and tracked. **(T-3)**

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Air Force Deputy Chief Information Officer (SAF/CN).

2.1.1. Work with the Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance and Cyber Effects Operations (AF/A2/6) on policy development and implementation of AF cybersecurity workforce requirements and processes. Interpret and promulgate cybersecurity workforce directives, policies and requirements (e.g., DoD 8570.01-M).

2.1.1.1. Provide direction on positions' determinations for the cybersecurity workforce.

2.1.1.2. Coordinate with AF/A2/6 on updates to the Enlisted and Officer Classification Directories to reflect SEI requirements for the cybersecurity workforce.

2.1.1.3. Provide direction on reporting metrics on the cybersecurity workforce.

2.1.1.4. Work with AF/A2/6 to provide programming and budget guidance to MAJCOMs for cybersecurity workforce management, to include certification exam and maintenance fee costs, and computer-based training.

2.1.1.5. Provide direction on annual validations of the cybersecurity workforce.

2.1.1.6. Provide direction on supplemental cybersecurity workforce training.

2.1.1.7. Ensure reasonable accommodations for military and civilian personnel in accordance with AFI 36-205, *Affirmative Employment Programs, Special Emphasis Programs, and Reasonable Accommodation Policy*.

2.1.2. Oversee the AF Cybersecurity Workforce Improvement Program and distribution of certification funds for the AF.

2.1.3. Identify, track, and monitor AF cybersecurity personnel and qualifications, including certifications.

2.1.4. Collect and report on metrics and submit consolidated reports to the DoD CIO, standardizing reporting across the AF.

2.1.5. Track Authorizing Official-signed certification waivers, as discussed in **Chapter 8**.

2.1.6. Participate as member on various DoD cybersecurity workforce forums and groups.

2.1.7. Assist certification providers with AF policy when applying to use the .mil network to proctor electronic certification exams (e.g., assess software needed by the education offices using .mil).

2.1.8. Assist AF/A2/6 with integrating institutional education and training programs and requirements (i.e., ancillary, Professional Military Education [PME], and accessions) into the appropriate venues prior to levying on the Total Force. Career field specific requirements are coordinated with the respective career field manager for integration into Career Field Training and Education Plan, Specialty Training Standard, or Course Training Standard, as appropriate.

2.1.9. Acquire capability for Program Management Offices (PMOs) or units to track and manage qualifications of AF cybersecurity workforce.

2.1.10. Update skill-awarding and supplemental courses for the cyber workforce to facilitate gaining certification upon course completion, if cost-benefit analysis supports such action.

2.1.11. Ensure Air Education and Training Command has the most current DoD approved annual cybersecurity user awareness training product(s).

2.1.12. Work with AF/A2/6, Deputy Chief of Staff of the AF, Manpower, Personnel and Services (AF/A1), and the Assistant Secretary of the AF, Acquisition, Technology, & Logistics (SAF/AQ) on a capability to automate reporting of the AF cybersecurity workforce (e.g., qualification status).

2.2. Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance and Cyber Effects Operations (AF/A2/6)

2.2.1. Work with the SAF/CN to develop policy and direct implementation of AF requirements and processes. Interpret and promulgate cybersecurity workforce directives, policies and requirements (e.g., DoD 8570.01-M).

2.2.1.1. Oversee updates to the Enlisted and Officer Classification Directories to reflect SEI requirements for the cybersecurity workforce.

2.2.1.2. Work with SAF/CN to provide programming and budget guidance to MAJCOMs for cybersecurity workforce management and improvement programs to include certification exam and maintenance fee costs, and computer-based training.

2.2.1.3. Ensure reasonable accommodations for military and civilian in accordance with AFI 36-205.

2.2.2. Participate as member on various DoD cybersecurity workforce forums and groups. **(T-0)**

2.2.3. Oversee the integration of institutional education and training programs and requirements (i.e., ancillary, PME, and accessions) into the appropriate venues for the Total Force. Career field specific requirements are coordinated with the respective career field manager for integration into Career Field Training and Education Plan, Specialty Training Standard, or Course Training Standard, as appropriate.

2.3. Deputy Chief of Staff of the Air Force, Manpower, Personnel and Services (AF/A1).

2.3.1. Provide a capability to identify, record and track civilian and military cybersecurity positions via SEIs on the UMD in accordance with DoD 8570.01-M and **Paragraph 1.3.4**. **(T-0)**

2.3.2. Provide a capability to identify and track civilian and military cybersecurity personnel.

2.3.3. Provide advice on union representation related to cybersecurity workforce requirements (e.g., certifications, positions).

2.3.4. Ensure guidance is provided to support human resources (HR) agencies for management of cybersecurity workforce within manpower and personnel databases or systems.

2.4. Assistant Secretary of the Air Force, Acquisition, Technology & Logistics (SAF/AQ).

2.4.1. Ensure acquisition strategies as well as contracts for Information Systems and PIT Systems address cybersecurity workforce requirements.

2.4.2. Ensure programs budget for certified and qualified cybersecurity personnel to support Co systems throughout life cycles.

2.4.3. Work with AF/A1, AF/A2/6, and SAF/CN on a capability to automate reporting of the AF cybersecurity workforce (e.g., qualification status).

2.5. Director of Security, Special Programs Oversight (SAF/AAZ). Track the compliance data of Special Access Program Information Systems and PIT Systems with cybersecurity workforce requirements.

2.6. Air Force Career Field Manager(s).

2.6.1. Will periodically review AFSC(s) or occupational series and certification level for inclusion or removal in the cybersecurity workforce program. **(T-1)**

2.6.2. Will ensure enlisted and officer classification directories are updated with SEIs for tracking cybersecurity workforce requirements or certifications for the AFSC(s) the Career Field Manager manages. **(T-1)**

2.6.3. Will ensure civilian position description guidance is provided for tracking cybersecurity workforce requirements or certifications for applicable occupational series. **(T-1)**

2.7. MAJCOMs.

2.7.1. Provide oversight over the cybersecurity workforce, ensuring workforce is identified, trained, certified, qualified, tracked, and managed in accordance with DoD and AF Cybersecurity Workforce Improvement Program directives and policies (e.g., DoDD 8140.01, DoD 8570.01-M, and this manual). **(T-0)**

2.7.2. Ensure the cybersecurity workforce positions are reviewed periodically and validated annually in accordance with SAF/CN guidance (e.g., template and suspense dates).

2.7.3. Act as the command focal point (or equivalent) on cybersecurity workforce issues.

2.7.4. Consolidate base or wing reporting inputs on civilian, military, and contractor cybersecurity workforce metrics.

2.7.5. Report the status of their cybersecurity workforce metrics to SAF/CN, as directed. An example report is provided in **Attachment 4**.

2.8. Air Combat Command.

2.8.1. Collect, monitor, and analyze data in support of program management actions.

2.8.2. Submit Program Objective Memorandum for AF-wide training and tracking of approved civilian and military cybersecurity workforce authorizations.

2.8.3. Supplement formal training programs with commercial cybersecurity training as needed.

2.8.4. Provide on-line training materials via AF e-learning website available through the Air Force Portal.

2.8.5. Publish information regarding AF-endorsed certification requirements.

2.8.6. Execute the AF 8570 Program funds for preferred certifications and maintenance fees.

2.9. Air Education and Training Command.

2.9.1. Provide and sustain availability of cybersecurity user awareness training provided by the SAF/CN.

2.9.2. Provide schoolhouse training, certification testing, and cybersecurity user awareness training to students (civilian, military and foreign military) as appropriate.

2.10. Air Force Personnel Operations Agency.

2.10.1. Upon request, will extract reports from manpower and personnel databases or systems (e.g., Military Personnel Data System and DCPDS) to identify cybersecurity workforce certification requirements and certified personnel for AF compliance reporting. **(T-1)**

2.10.2. Upon request, will provide technical assistance to the AF/A2/6 and SAF/CN on manpower and personnel systems (e.g., data field entries). **(T-1)**

2.11. Air Force Personnel Center.

2.11.1. Upon the request of the appropriate AF/A2/6 Career Field Manager, update the AF Enlisted Classification Directory (AFECD) or AF Officer Classification Directory (AFOCD) with SEIs to track the military cybersecurity workforce. **(T-1)**

2.11.2. Confirm approved changes in cybersecurity certification completion for civilian personnel are updated in civilian personnel database(s) or system(s). **(T-1)**

2.11.3. Confirm approved changes in cybersecurity certification completion for military personnel are updated in military personnel database(s) or system(s). **(T-1)**

2.12. Authorizing Officials.

2.12.1. Comply with cybersecurity training requirements in accordance with **Paragraph 3.2.4** **(T-0).** The DoD Authorizing Official training is located at this link the DoD Cyber Exchange NIPR portal (Common Access Card-enabled): **https://cyber.mil/training/dod-authorizing-official-ao/**.

2.12.2. Provide oversight over cybersecurity personnel and positions, including the certification exemption process stated in **Paragraph 3.2.11,** supporting responsible Information Systems and PIT Systems. **(T-1)**

2.12.3. Provide oversight over the DoD approved cybersecurity baseline certification waiver process in accordance with **Chapter 7**. **(T-1).** These waivers are only applicable to cybersecurity-related positions under the Authorizing Official's authority.

2.13. Wing Cybersecurity Office (WCO).

2.13.1. Will monitor status on all Wing cybersecurity workforce personnel. **(T-1)**

2.13.2. Will report status on all Wing cybersecurity workforce personnel to MAJCOM. **(T-1).** An example report is provided in **Attachment 4**.

2.13.2.1. Will collect the UMD position validation status from units. **(T-1)**

2.13.2.2. Will collect qualification status data from units. **(T-1)**

2.13.2.3. Will collect contractor status data from units. **(T-1)**

2.13.3. Will serve as focal point for the Wing's implementation of AF 8570 policies. **(T-2)**

2.13.4. Will ensure the cybersecurity workforce positions are reviewed periodically and validated annually in accordance with SAF/CN guidance. **(T-1)**

2.13.5. Will consolidate unit reporting inputs on civilian, military, and contractor cybersecurity workforce metrics. **(T-2)**

2.14. Program or Project Managers (PMs), System Managers, Program Management Offices (PMOs), Developmental or Operational Test Agencies, and Units.

2.14.1. Will identify, track and manage all cybersecurity workforce positions **(T-0)**. A position, regardless of AFSC, job title, occupational series, or contractor job title, must perform one or more cybersecurity tasks to be part of the DoD cybersecurity workforce in accordance with DoD 8570.01-M. **(T-0)**. You are required to follow Attachment 2, Air Force Cybersecurity Workforce Position Certification Determination guide related to task identified in Table A2.1. Technical Category, to assist with determining the Information Assurance Technical level actions.

2.14.1.1. Will ensure every civilian and military with privileged accounts are assigned to a cybersecurity-coded positions on the UMD **(T-0)**

2.14.1.2. Will identify all civilian and military cybersecurity positions in manpower and personnel databases or systems. **(T-0)**

2.14.2. Will ensure all cybersecurity workforce personnel are certified and qualified in accordance with DoD 8570.01-M and this manual. **(T-0)**

2.14.2.1. Will verify every civilian and military with privileged accounts are assigned to a cybersecurity-coded positions on the UMD. **(T-0)**

2.14.2.2. Will verify every civilian and military personnel have signed a formal statement of assigned cybersecurity responsibilities. **(T-0).** The formal statements of assigned cybersecurity responsibilities will be maintained locally. **(T-0).** Suggested formats can be found in **Attachment 5.**

2.14.3. Will review the UMD to ensure all civilian and military positions are identified and recorded with the appropriate SEI. **(T-1).** Identify positions to be updated and notify the servicing manpower office to update the SEI on the UMD. **(T-1)**

2.14.3.1. Will initiate corrective actions, when necessary, to implement the requirements described within this manual **(T-1).**

2.14.3.2. Will ensure the servicing Civilian Personnel Section and position classification activity or section are notified of any changes to civilian positions in the cybersecurity workforce. **(T-2)**

2.14.4. Will ensure personnel in all cybersecurity workforce positions possess the appropriate clearance or national security investigation for position in accordance with DoD 8570.01-M, Paragraph C1.4.4.6.4. **(T-0).** Will not approve or initiate privileged requests for an Information System or PIT System until individual possesses the appropriate clearance or national security investigation. **(T-0)**

2.14.5. Will ensure civilian core personnel documents or position descriptions reflect accurately the cybersecurity workforce requirements. **(T-0)**

2.14.6. Will only assign US citizens to IAT Category Level III, IAM Category Level III, and IASAE Specialty Level III positions in accordance with DoD 8570.01-M. **(T-0)**

2.14.7. Will take appropriate actions in accordance with **Paragraph 5.6** on military and civilian personnel in cybersecurity workforce positions when DoD approved cybersecurity baseline certifications are not achieved within six (6) months of filling the position, a baseline certification has expired, an individual has become decertified, or baseline certification waivers (see **Chapter 7**) are not obtained. **(T-0)**

2.14.8. Will conduct an annual validation of civilian and military cybersecurity workforce positions on the UMD and the data in personnel databases or systems (e.g., DCPDS for civilians and Military Personnel Data System for military). **(T-1).**

2.14.9. Will include all contractor cybersecurity requirements in new, renewed or modified contract and associated statement of work or performance work statement. **(T-0)**

2.14.9.1. Contractor cybersecurity requirements will include baseline certification category or specialty and level for contractor personnel. **(T-0)**

2.14.9.2. Will ensure contractor cybersecurity requirements are evaluated for position sensitivity using the Office of Personnel Management Position Designation Tool (available at **https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool**) as required by 5 CFR§1400. **(T-0)**

2.14.9.3. Will coordinate with the supporting Information Protection Office or equivalent office for submission of national security background investigations when contractor roles are identified as "sensitive positions" without a requirement for access to classified information. **(T-0)**

2.14.9.4. Will coordinate with the Contracting Officer to ensure security background investigation and clearance requirements (when appropriate) are incorporated into the contract and associated statement of work or performance work statement. **(T-0)**

2.14.9.5. Will notify Contracting Officer whenever contractor cybersecurity requirements must be added or modified. **(T-0)**

2.14.10. Will verify all contractor personnel meet contract cybersecurity requirements (e.g., initial and annual cybersecurity awareness training, DoD approved cybersecurity baseline certification, annual training for non-senior software development role). **(T-0)**

2.14.10.1. Will verify all contractor personnel have valid DoD approved cybersecurity baseline certification(s) prior to supporting any cybersecurity tasks on new, renewed, or modified contract. **(T-0)**

2.14.10.2. Will verify only US citizens fill contractor roles as an IAT Category Level III, IAM Category Level III, and IASAE Specialty Level III in accordance with DoD 8570.01-M. (**T-0)**

2.14.10.3. Will verify all contractor personnel maintain valid DoD approved cybersecurity baseline certification(s). **(T-0)**

2.14.10.4. Will report DoD approved cybersecurity baseline certification statuses of contractor personnel to the Contracting Officer or designated representative. **(T-1)**

2.14.11. Will confirm all contractor personnel complete or sign a formal statement of assigned cybersecurity responsibilities. **(T-0)**

2.14.11.1. The formal statements of assigned cybersecurity responsibilities will be maintained locally. **(T-0)**

2.14.11.2. The formal statement will be added as a Contract Data Requirement List (CDRL) deliverable. **(T-1)**. A suggested format can be found in **Attachment 6** for contractors.

2.14.12. Will coordinate with the Contracting Officer the immediate removal of contractor personnel who do not meet or maintain required DoD approved cybersecurity baseline certification(s) in accordance with contract cybersecurity requirements. **(T-0)**

2.14.13. Will coordinate with the Contracting Officer the immediate removal of contractor personnel who perform non-senior software development roles, but do not meet annual training requirement as specified in **Paragraph 3.2.12.2.2.1**. **(T-1)**

2.14.14. Will not initiate certification waivers for contractors in accordance with DoD 8570.01-M, Paragraph C2.3.9. **(T-0)**

2.14.15. Will collect cybersecurity workforce (civilian, military, and contractor) cybersecurity workforce metrics. **(T-1)**

2.14.16. Will report cybersecurity workforce (civilian, military, and contractor) metrics or statistics to WCO, as required. **(T-0).** SAF/CN will provide the instructions (e.g., reporting requirements, criteria, template, and reporting frequency). **(T-1). Attachment 4** lists an example metric format. At present, AF does not have a centralized or consolidated database or system to track contractor cybersecurity requirements. Therefore, contractor requirements must be tracked locally. **(T-1)**

2.14.17. Will ensure all civilian and military cybersecurity positions are reviewed periodically. **(T-1)**

2.15. Contracting Officer.

2.15.1. Will confirm Defense Federal Acquisition Regulation Supplement 252.239-7001 clause is included in every solicitation or contract involving contractor performance of cybersecurity functions in accordance with DoD 8570.01-M. **(T-0)**

2.15.2. Will immediately notify contractor (private sector) company to stop any contractor employee from performing any cybersecurity-related work under a government contract when that contractor employee does not meet or maintain required DoD approved cybersecurity baseline certification(s). **(T-0).** Contractors will be ineligible for certification baseline waivers as described in **Chapter 7**. **(T-0)**

2.15.3. Will immediately notify contractor (private sector) company to stop any contractor employee from performing on a government contract if the contractor employee is in a non-senior software development role and does not meet annual training requirement as specified in **Paragraph 3.2.12.2.2.1** **(T-1)**

2.16. Information System Security Managers (ISSMs).

2.16.1. Will validate an individual has signed a Privileged User Agreement, completed the appropriate clearance or national security investigation appropriate for access, and possessed required DoD approved cybersecurity baseline certification(s) before a privileged account to Information System or PIT System is granted. **(T-2)**

2.16.2. Will track Privileged User Agreements for each responsible Information System or PIT System. **(T-2).** Provide updates to the Authorizing Official or WCO, directed.

2.16.3. Will ensure the cybersecurity workforce certification and training of Information Systems or PIT Systems meets compliance for mission readiness and management review items. **(T-2)**

2.17. Civilian Personnel Section.

2.17.1. Will process personnel action requests (e.g., Authorization Change Requests [ACRs]) to identify cybersecurity workforce requirements within appropriate personnel database(s) or system(s). **(T-2)**

2.17.2. Will ensure information is forwarded to the servicing classification office for review and appropriate action, to include updating personnel data systems and, if necessary, updating core personnel document and position classification. **(T-2)**

2.17.3. Will work with the Labor Relations Officer or equivalent to confirm collective bargaining obligations are met. **(T-2)**

2.18. Supervisors.

2.18.1. Will incorporate cybersecurity certification and qualification requirements in accordance with **Chapters 4** and **5** within the Master Training Plan and training documentation for cybersecurity workforce. **(T-3)**

2.18.2. Will ensure personnel identified in the cybersecurity workforce are prepared to obtain and maintain qualifications. **(T-3)**

2.18.3. Will confirm civilians and military complete or sign a formal statement of assigned cybersecurity responsibilities. **(T-0). Attachment 5** lists examples of a formal statement.

2.18.4. Will ensure the member is earning continuing educational units as required by the commercial provider to maintain DoD approved cybersecurity baseline certification in good standing. **(T-3)**

2.18.5. Will approve certification exam requests only for eligible civilian and military personnel in coded cybersecurity workforce positions who are not within one (1) year of a confirmed retirement or separation date. **(T-0)**

2.18.6. Will validate civilian and military personnel have completed, if applicable, the appropriate computing environment or operating system training in accordance with **Paragraph 4.2** for assigned task(s). **(T-0)**

2.19. Individuals (Civilian and Military).

2.19.1. Will obtain appropriate DoD approved cybersecurity baseline certification(s) applicable for cybersecurity tasks required for the DoD position held, within six months of filling position in accordance with DoD 8570.01-M, Paragraphs C3.2.4.1.1, C4.2.3.2, C10.2.3.2, and C11.2.4.1.1. **(T-0)**

2.19.2. Will maintain valid (i.e., in good standing) DoD approved cybersecurity baseline certification(s) in accordance with DoD 8570.01-M, Paragraph C2.3.7. **(T-0).** Please see **Paragraph 5.7** for more details on continuing education units and maintenance fees. Also, please see **Paragraph 5.6** for more details on failure to obtain or maintain required baseline certification(s).

2.19.3. Will become qualified in cybersecurity position as defined in **Chapter 4. (T-0)**

2.19.4. Will sign a formal statement of assigned cybersecurity responsibilities in accordance with DoD 8570.01-M, Paragraphs C3.2.4.4, C4.2.3.6, and C10.2.3.6. **(T-0) Attachment 5** lists an example of a formal statement.

2.19.5. Will sign a Privileged User Agreement for every privileged account assigned in accordance with DoD 8570.01-M, Paragraph C2.1.4. **(T-0).** An example agreement can be found in DoD 8570.01-M, Appendix 4.

2.19.6. Will authorize release of DoD approved cybersecurity baseline certification data to DoD in accordance with DoD 8570.01-M, Paragraphs C2.3.12. **(T-0).** Personnel can access and submit release authorization at this link: **https://cyss.us.af.mil/cyss/certifiedworkforce/**. **(T-1)**

2.19.7. Will report Continuing Education Units (CEUs) or Continuing Professional Education (CPE) status to supervisor. **(T-0)**

2.20. Individuals (Contractor Personnel).

2.20.1. Will obtain appropriate cybersecurity certification(s) applicable for assigned cybersecurity workforce position prior to start of contractual tasks in accordance with DoD 8570.01-M, Paragraph C2.3.9. **(T-0)**

2.20.2. Will maintain valid (i.e., in good standing) DoD approved cybersecurity baseline certification(s) in accordance with DoD 8570.01-M, Paragraph C2.3.7. **(T-0).** Please see **Paragraph 5.7** for more details on continuing education units and maintenance fees.

2.20.3. Will become qualified in cybersecurity contractor position as defined in **Chapter 4. (T-0)**

2.20.4. Will sign a formal statement of assigned cybersecurity responsibilities in accordance with DoD 8570.01-M, Paragraphs C3.2.4.4, C4.2.3.6, and C10.2.3.6. **(T-0)**

2.20.5. Will sign a Privileged User Agreement for every privileged account assigned in accordance with DoD 8570.01-M, Paragraph C2.1.4. **(T-0).** An example agreement can be found in DoD 8570.01-M, Appendix 4.

2.20.6. Will authorize release of DoD approved cybersecurity baseline certification data to DoD in accordance with DoD 8570.01-M, Paragraphs C2.3.12. **(T-0).** Personnel can access and submit release authorization at this link: **https://cyss.us.af.mil/cyss/certifiedworkforce/**. **(T-1)**

2.20.7. Will not be eligible for DoD approved cybersecurity baseline certification waivers in accordance with DoD 8570.01-M, Paragraphs C2.3.9. **(T-0)**

Chapter 3

CYBERSECURITY WORKFORCE IDENTIFICATION

3.1. Position Identification. Supervisors and managers will review all manpower positions, duty descriptions, or contract requirements to determine if cybersecurity tasks are required to be performed by that position in accordance with DoD 8570.01-M, Chapters 3, 4, 5, 10, and 11. **(T-0).** Please refer to **Attachment 2**, to assist supervisors in the identification process. If a civilian or military position is identified as part of the cybersecurity workforce, then the supervisor will record requirement, and the assigned individual will obtain the appropriate certification commensurate with the position. **(T-0).** If a position has assigned cybersecurity tasks spanning across one or more levels within a category or specialty, then assigned individual will obtain the appropriate certification(s) for the highest level within a category or specialty in accordance with DoD 8570.01-M, Paragraph C2.2.5. **(T-0).** Supervisors should try to consolidate positions with assigned cybersecurity tasks as an additional duty (assigned cybersecurity task[s] amount to 15 to 24 hours weekly) or an embedded duty (assigned cybersecurity task[s] amount to up to 14 hours weekly) maximizing resources. For additional duty guidance, review AFI 38-206, *Additional Duty Management*. Likewise, supervisors should try to limit the number of individuals requiring privileged accounts to the minimum necessary to support mission tasks.

3.2. Cybersecurity Workforce. The AF cybersecurity workforce (civilian, military, or contractor) will obtain and maintain DoD approved cybersecurity baseline certification(s) for assigned UMD position (civilian and military) or contract requirement (contractor) in accordance with DoD 8570.01-M, Paragraphs C2.3.2. **(T-0).** The list of DoD approved cybersecurity baseline certifications can be found at this link on the DoD Cyber Exchange NIPR portal (Common Access Card-enabled): **https://cyber.mil/cwmp/dod-approved-8570-baseline-certifications/**. Civilians and military personnel will obtain required DoD approved cybersecurity baseline certification within six (6) months of formal assignment of cybersecurity tasks, except as noted in **Paragraph 3.2.12** for software developers, engineer, or programmers. **(T-0).** The AF cybersecurity workforce is grouped predominately by category (IAT and IAM) or specialty (CSSP and IASAE). The categories and specialties are subdivided further into levels, related to functional skill requirements or system environment focus. Please refer to **Attachment 2** for breakout of cybersecurity tasks to be performed by each category or specialty and level.

3.2.1. Information Assurance (IA) Technical (IAT) Category. An IAT position is defined as anyone who has been given access rights to manage core or DoD Information Networks Operations (DoDIN Ops) service(s), servers, or end-point devices. Core or DoDIN Ops services include but are not limited to the following: messaging or email services, directory services, application or web hosting services, vulnerability management, network boundary management, etc.

3.2.1.1. IAT Level I. An IAT Level I position is focused primarily on the secure operation of client-level workstations or end user devices (i.e., mobile device, laptop, etc.). As such, the impacts of IAT Level I tasks are limited to client-level workstations or end user devices, their operating systems, peripherals, and applications. For instance, an IAT Level I task could be to correct anomalies or vulnerabilities. Another example IAT Level I task would be to implement security controls in the hardware or software installed. Examples of IAT Level I include a technician who is responsible for patching end-user devices, a technician who is supporting an Internet Protocol -managed land mobile radio networks and an individual who performs AF Network (AFNET) user account management tasks.

3.2.1.2. IAT Level II. An IAT Level II position provides networked environment support. Also, the IAT Level II is focused on intrusion detection, finding and fixing unprotected vulnerabilities, and conducting vulnerability scans. Examples of IAT Level II include a technician who installs servers, technician who maintains routers and switches, and personnel who are creating or modifying privileged accounts.

3.2.1.3. IAT Level III. An IAT Level III position is responsible for incident response and making technical decisions regarding the cybersecurity posture of the enterprise. Examples of IAT Level III include a Security Control Assessor Representative who performs mostly technical assessments or audits and a technician who maintains and upgrades core service network devices (e.g., Information Transfer Nodes, Service Delivery Point Routers, Primary Domain Controllers).

3.2.2. IA Management (IAM) Category. An IAM Category position is defined as anyone who has oversight of cybersecurity programs or tasks involving management decisions for the administration of core or DoDIN Ops service(s), network devices, servers or end-point devices. Core or DoDIN Ops services included but are not limited to the following: messaging or email services, directory services, application or web hosting services, vulnerability management, network boundary management, etc. An individual possessing an IAM certification typically does not have a privileged account or require computing environment or operating system certification.

3.2.2.1. IAM Level I. An IAM Level I position is responsible for the implementation and operation of a DoD Information System (IS) or system DoD component within their Computing Environment (CE). Examples of an IAM Level I position include select cyber crew commanders and WCO staff, except for the Base or Wing ISSM.

3.2.2.2. IAM Level II. An IAM Level II position is responsible for the Information Assurance program of an IS within the network environment. An example of an IAM Level II position is the Base or Wing ISSM.

3.2.2.3. IAM Level III. An IAM Level III position is responsible for ensuring that all enclave Information Systems are functional and secure. Examples of an IAM Level III position include the AF Chief Information Security Officer (CISO), select AF CISO staff personnel, Security Control Assessor, and ISSM For Information Systems and PIT Systems providing enterprise capabilities or operating across multiple networking environments (e.g., AFNET or AF Network Secure [AFNET-S], Civil Engineering Industrial Control System Virtual Local Area Network, etc.).

3.2.3. AF Chief Information Security Officer (CISO). The AF CISO is the official responsible for directing the AF's cybersecurity program on behalf of the AF CIO. The AF CISO will obtain and maintain a DoD approved IAM Level III cybersecurity baseline certification. **(T-1).** The AF 8570 Program will pay for certification exam and associated maintenance fees. **(T-1)**

3.2.4. Authorizing Official. The Authorizing Official is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. In accordance with DoD 8570.01-M, Paragraph C5.3.1.1, the Authorizing Official will complete a DoD mandated Authorizing Official training module within 60 days of assignment. **(T-0).** The Authorizing Official position does not have a mandatory DoD approved cybersecurity baseline certification.

3.2.5. Cybersecurity Risk Management Roles.

3.2.5.1. Authorizing Official Designated Representative (AODR). In accordance with AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* an Authorizing Official can appoint an AODR to assist in managing the life-cycle cybersecurity risks to Information Systems or PIT Systems. The AODR can serve as technical support for Authorizing Official as well as act on behalf of the Authorizing Official for all duties except the acceptance of risk. The AODR will complete a DoD mandated Authorizing Official training module. **(T--1).** The AODR position could be assigned cybersecurity tasks that may require obtaining or maintaining a DoD approved cybersecurity baseline certification. For instance, an AODR could be assigned as a Security Control Assessor.

3.2.5.2. Security Control Assessor. The Security Control Assessor is a role where the senior official having the authority and responsibility for leading the evaluation of security controls for an Information System or PIT System. The Security Control Assessor roles and responsibilities are addressed in AFI 17-101. SCAs will obtain and maintain a DoD approved IAM Level III DoD approved cybersecurity baseline certification. **(T-1).** Also, it is highly recommended SCAs should complete the Authorizing Official training module and supplemental training on the Authorizing Official responsibilities, security program management, and security risk analysis or mitigation.

3.2.5.3. Security Control Assessor Representative (SCAR). SCARs is a position or role to assist SCAs in the evaluation of security controls for an Information System or PIT System. SCARs will obtain and maintain a Level III DoD approved cybersecurity baseline certification commensurate to assigned position **(T-1).** The SCAR position or role will be classified as either an IAM Level III or IAT Level III. **(T-1).** The Authorizing Official can designate the SCAR as an IAT Level III position if the SCAR is performing predominately technical tasks (e.g., assessment or validation of security controls). Otherwise, the Authorizing Official can designate the SCAR as an IAM Level III position. Also, it is highly recommended SCARs should complete the Authorizing Official training module and obtain supplemental training on the Authorizing Official responsibilities, security program management, and security risk analysis or mitigation.

3.2.6. IA System Architect and Engineer (IASAE) Specialty. In accordance with DoD 8570.01-M, Table C10.T1., IASAE positions (all levels) will obtain and maintain an IA baseline certification. **(T-0)**

3.2.6.1. IASAE Level I. An IASAE Level I position is responsible for the design, development, implementation, or integration of a DoD Information System or PIT System cybersecurity architecture, system, or system component for use. Examples include Information System Security Engineers (ISSEs) supporting standalone or point-to-point systems, as well as, supporting only the client or endpoint components of a larger Information System or PIT System.

3.2.6.2. IASAE Level II. An IASAE Level II position is responsible for the design, development, implementation, or integration of a DoD cybersecurity architecture, system, or system component for use within the Network Environment. Examples include ISSEs supporting functional-level systems connected to the DoDIN, but where adverse impacts can be isolated to only those who are interconnected.

3.2.6.3. IASAE Level III. An IASAE Level III position is responsible for the design, development, implementation, or integration of a DoD cybersecurity architecture, system, or system component for use within enterprise environments. They ensure that the architecture and design of DoD Information Systems or PIT System(s) are operational and secure. Examples include ISSEs supporting enterprise-level (irrespective of functional community) Information System(s) connected to the DoDIN.

3.2.7. Cyber Security Service Provider (CSSP) Specialty Positions. CSSP Specialty Positions are predominately located within organization(s), providing one or more cybersecurity services to implement and protect the AFIN.

3.2.7.1. CSSP Analyst (CSSP-A). A CSSP-A uses data collected from a variety of cyber tools (including intrusion detection system alerts, firewall and network traffic logs, and host system logs) to analyze events that occur within their environment. An individual in a CSSP-A position will obtain and maintain both an IAT DoD approved cybersecurity baseline certification and a CSSP-A Specialty cybersecurity certification commensurate to assigned UMD position (civilian and military) or contract requirement (contractor). **(T-0)**

3.2.7.2. CSSP Auditor (CSSP-AU). A CSSP-AU performs assessments of systems and networks within the Network Environment or enclave and identify where those systems or networks deviate from acceptable configurations, enclave policy, or local policy. An individual in a CSSP-AU position will obtain and maintain both an IAT DoD approved cybersecurity baseline certification and a CSSP-AU Specialty DoD approved cybersecurity certification commensurate to assigned UMD position (civilian and military) or contract requirement (contractor). **(T-0)**

3.2.7.3. CSSP Incident Responder (CSSP-IR). A CSSP-IR investigates and analyzes all response activities related to cyber incidents. An individual in a CSSP-IR position will obtain and maintain both an IAT DoD approved cybersecurity baseline certification and a CSSP-IR Specialty cybersecurity certification commensurate to assigned UMD position (civilian and military) or contract requirement (contractor). **(T-0)**

3.2.7.4. CSSP Infrastructure Support (CSSP-IS). A CSSP-IS tests, implements, deploys, maintains, and administers the infrastructure assets or equipment which are required to effectively manage the cybersecurity provider network and resources. Assets may include, but is not limited to routers, firewalls, and intrusion detection or prevention systems. An individual in a CSSP-IS position will obtain and maintain both an IAT DoD approved cybersecurity baseline certification and a CSSP-IS Specialty cybersecurity certification commensurate to assigned UMD position (civilian and military) or contract requirement (contractor). **(T-0)**

3.2.7.5. CSSP Manager. A CSSP Manager oversees the cybersecurity service provider tasks. A CSSP Manager is responsible for producing guidance, assisting with risk assessments and risk management, and managing the technical classification. An individual in a CSSP Manager position will obtain and maintain both an IAM DoD approved cybersecurity baseline certification and a CSSP Manager Specialty cybersecurity certification commensurate to assigned UMD position (civilian and military) or contract requirement (contractor). **(T-0)**

3.2.8. System Information System Security Managers (ISSMs). A system ISSM for an Information System or PIT System creates or oversees the cybersecurity program to include cybersecurity architecture, requirements, personnel, policies, processes and procedures. Acting as the primary cybersecurity technical advisor to the Authorizing Official for an Information System or PIT System, it is imperative that the system ISSM have the appropriate foundational knowledge of cybersecurity best practices and risk management commensurate to the criticality of information stored or processed on the Information Systems and PIT Systems. For Information Systems and PIT Systems providing enterprise capabilities or operating at the AFIN level, the system ISSM will obtain and maintain, at a minimum, an IAM Level III DoD approved cybersecurity baseline certification. **(T-1).** For all remaining Information Systems and PIT Systems, the system ISSM will obtain and maintain, at a minimum, an IAM Level II DoD approved cybersecurity baseline certification. **(T-1).** Roles and responsibilities of ISSMs are addressed in AFI 17-101 and AFI 17-130).

3.2.9. Information System Security Officers (ISSOs). For Information Systems and PIT Systems providing enterprise capabilities or services to AF end users worldwide, the ISSO will obtain and maintain an IAT Level III DoD approved cybersecurity baseline certification. **(T-1).** Otherwise, the ISSO position will obtain and maintain, at a minimum, an IAT Level II DoD approved cybersecurity baseline certification. **(T-1).** Roles and responsibilities of ISSOs are addressed in AFI 17-101 and AFI 17-130).

3.2.10. Privileged Users. The Committee on National Security Systems Instruction 4009, *Committee on National Security Systems Glossary*, defines a "privileged user" as a user that is authorized to have elevated network rights to perform security-relevant tasks that ordinary users are not authorized to perform. For an unsupervised privileged account, every individual will obtain and maintain a DoD approved cybersecurity baseline certification as defined by assigned UMD position (civilian and military) or contract requirement (contractor). **(T-1).** For supervised privileged account, users will be under the direct supervision (i.e., guidance and observation) of an individual who possess a DoD approved cybersecurity baseline certification. in accordance with in accordance with DoD 8570.01-M, Paragraph AP1.22**,** an individual who has access to system control, monitoring or security, administration, criminal investigation or compliance tasks to an Information System or PIT System must be classified as an AF "privileged user," except for exemption specified in **Paragraph 3.2.11** **(T-1)**

3.2.10.1. A temporary unsupervised privileged account may be granted due to mission requirements while an individual achieves a DoD approved cybersecurity baseline certification commensurate to UMD requirements. Even with a certification waiver (described in **Chapter** 7), a temporary unsupervised privileged account will not be granted unless the individual possesses a DoD approved cybersecurity baseline certification in good standing in accordance with in accordance with DoD 8570.01-M, Paragraph C3.2.4.1.2. **(T-1)**

3.2.10.2. Personnel in training for a privileged account do not require a DoD approved cybersecurity baseline certification while under the direct supervision of a trainer. The trainer will possess in good standing a DoD approved cybersecurity baseline certification. **(T-1)**

3.2.11. Certification Requirement Exemption Process for Individuals Supporting Information System or PIT System. Cybersecurity is critical for ensuring information is protected and the Information System or PIT System meet the operational requirements as designed under any cyber situation. Select AF workforce personnel (e.g., aircrew, maintenance, and system technicians) may need limited elevated permissions to perform tasks as required by AF publications (e.g., technical orders, aids, software handbooks, checklists, and contractor-developed technical manual procedures) to facilitate operation, troubleshooting, and repair of Information System or PIT System. Limited elevated permissions are elevated network rights for a specific requirement as required by AF publications, but do not include all of the permissions of a privileged user. These tasks may not require training, certifications, or qualifications beyond the requirements established in publications such as mission design series documents and technical orders. These AF publications have been vetted and approved by the responsible Authorizing Official to prevent the unauthorized alteration of an Information System or PIT System's cybersecurity posture. An Authorizing Official can make a certification requirement determination, exempting individuals who have limited elevated network or system permissions to an Information System or PIT System. The determination must apply only to Information System or PIT System(s) under the Authorizing Official's authority and responsibility for risk acceptance **(T-1).** The PM will initiate the exemption determination memo, then ISSM will coordinate on the memo, and the Authorizing Official will sign the memo. **(T-1)**

3.2.11.1. The PM will ensure the exemption determination memo includes the following items:

3.2.11.1.1. General description of specific Information System or PIT System. **(T-1)**

3.2.11.1.2. Details on specific positions, including AFSCs or occupational series to be exempted **(T-1)**

3.2.11.1.3. Rationale why a DoD approved cybersecurity baseline certification is not required. **(T-1)**

3.2.11.1.3.1. Details on specific actions to be performed by individual as required by AF publications that necessitate limited elevated permissions. **(T-1)**

3.2.11.1.3.2. Details on security risk mitigations implemented to enable limited permissions. **(T-1).** Details should include reference info of AF publications (e.g., Technical Orders, aids, software handbooks, checklists, and contractor-developed technical manual procedures).

3.2.11.1.4. Statement(s) indicating the Authorizing Official has vetted and accepted risk as described in AF publications. **(T-1)**

3.2.11.1.5. Statement(s) describing process on how exempted personnel will be vetted initially and annually. **(T-1)**

3.2.11.1.6. Details on the specialized training and recurrence of exempted individuals. An example, personnel have to be recertified every "X" months on checklist procedures by 7-level evaluator or technician. **(T-1)**

3.2.11.1.7. Statement indicating exempted individuals sign a user agreement, stipulating the authorized actions or procedures to be performed. **(T-1)**

3.2.11.2. The PMO or functional system owner will maintain the exemption memo. **(T-1).** Also, for recordkeeping purposes, a copy of signed memo must be forwarded to the AF CISO for the affected Information System or PIT System. **(T-1)**

3.2.11.3. Exempted individuals will sign a user agreement, stipulating the limited authorized actions or procedures to be performed. **(T-1).** The PMO or functional system owner will maintain and track these signed user agreements. **(T-1)**

3.2.11.4. Exempted individuals will be classified as "Authorized Users" on the approved network or system account request form (e.g., DD Form 2875, *System Authorization Access Request [SAAR]*). **(T-1)**

3.2.11.5. The PMO or unit must complete and document in memo format an annual validation, occurring on anniversary date of exemption approval, of exemption memo to include personnel and Information System or PIT System. **(T-1).** The ISSM will sign the memo and route to the MAJCOM and Authorizing Official for in-turn signatures. **(T-2)** The PMOs and units must maintain and track validation memos locally. **(T-2).** For recordkeeping, a copy of a signed validation letter must also be forwarded to the AF CISO for the affected Information System or PIT System **(T-1)**.

3.2.12. Software Developer, Engineer, or Programmer Supporting Information System or PIT System. A software developer, engineer, or programmer designs, creates, modifies, integrates, tests, or maintains computer applications, software, or specialized utility programs for use on AF networks or systems. It is critical cybersecurity is integrated into the development, sustainment, and disposal of AF data, networks and systems.

3.2.12.1. Civilian and Military

3.2.12.1.1. Senior Software Development Roles: The PMOs or units must identify and record positions as an IASAE Level II for those civilians and military who are performing a senior software developer role, senior software consultant or subject matter expert (SME) role, or senior software tester role in accordance with **Attachment 2**. **(T-1).** These individuals will possess a DoD approved cybersecurity baseline certification on the DoD approved list and should have at least four years of software development experience. The DoD approved certification must cover knowledge areas, in sufficient detail, of secure software development in keeping with the intentions of the Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013 Section 933 (Improvements in Assurance of Computer Software Procured by DoD). **(T-1).** The knowledge areas must include, but are not limited to, secure software requirements and design, secure coding techniques, and secure software deployment strategies. **(T-1).** The PMOs or units must comply by 1 July 2020 of for all affected positions to be coded as well as personnel certified. (**T-1**)**.** Table A2.5 includes a list of representative tasks for the senior software development roles.

3.2.12.1.2. Remaining Software Development Roles: Every civilian and military member performing in a software developer, engineer, or programmer role, but not in a senior software development role as described in **Paragraph 3.2.12.1.1**, will complete annual supplemental training. **(T-1)**

3.2.12.1.2.1. Effective 1 July 2020, affected civilian and military personnel will be required to complete 40 supplemental training hours annually. **(T-1)**

3.2.12.1.2.1.1. The supplemental training must include elements of cybersecurity as well as programming or software language. **(T-1)** The cybersecurity training must be in addition to annual cybersecurity user awareness training. **(T-1)** Suggested cybersecurity training topics: cybersecurity principles, cyber threats and vulnerabilities, or secure coding practices.

3.2.12.1.2.1.2. The PMO or unit have the flexibility to define supplemental training details (e.g. methods). Acceptable training methods include formal or classroom instruction, on-the-job training, and computer based or web-based training.

3.2.12.1.2.2. The PMO or unit must document and track successful completion of supplemental training. **(T-1).** The training documentation must be accessible locally. **(T-3)**

3.2.12.2. Contractors

3.2.12.2.1. Senior Software Development Roles: Effective 1 July 2020, all contracts (new, modified and beginning with a new option year) must include the stipulation that all contractors performing a senior software developer role, senior software consultant or subject matter expert (SME) role, or senior software tester role in accordance with **Attachment 2** will be classified as an IASAE Level II. **(T-1).** Table A2.5 includes a list of representative tasks for the senior software development roles. These contractors will possess a DoD approved cybersecurity baseline certification on the DoD approved list and should have at least four years of software development experience. **(T-1).** This certification must be in good standing. **(T-1).** . The DoD approved certification must cover knowledge areas, in sufficient detail, of secure software development in keeping with the intentions of the National Defense Authorization Act for Fiscal Year 2013, Section 933 (Improvements in Assurance of Computer Software Procured by DoD). **(T-1).** The knowledge areas must include, but are not limited to, secure software requirements and design, secure coding techniques, and secure software deployment strategies. **(T-1)**

3.2.12.2.2. Remaining Software Development Roles: Every contractor performing in a software developer, engineer, or programmer role, but not in a senior software development role as described in **Paragraph 3.2.12.2.1**, will complete annual supplemental training: **(T-1)**

3.2.12.2.2.1. The affected contractors will complete 40 supplemental training hours annually. **(T-1).** Effective 1 July 2020, affected contractors will be required to complete 40 supplemental training hours annually. **(T-1)**

3.2.12.2.2.1.1. This supplemental training must include elements of cybersecurity as well as programming or software language. **(T-1)** The cybersecurity training must be in addition to annual cybersecurity user awareness training. **(T-1).** Suggested cybersecurity training topics: cybersecurity principles, cyber threats and vulnerabilities, or secure coding.

3.2.12.2.2.1.2. The PMO or unit will review applicability of contractor proposed training and content topics. **(T-1).** The PMO or unit will forward applicability reviews to Contracting Officer. **(T-1)**

3.2.12.2.2.2. The PMO or unit will verify the applicable contractor(s) have completed annual supplemental training requirement. **(T-1)**

3.2.13. Wing Cybersecurity Office (WCO).

3.2.13.1. The Base or Wing ISSM will obtain and maintain at a minimum an IAM Level II DoD approved cybersecurity baseline certification. **(T-1)**

3.2.13.2. Wing Communications Security Office Accounts with Key Management Infrastructure Capabilities: Individuals (civilian, military, or contractor) in the client platform administrator and client platform security officer roles must obtain and maintain, at a minimum, an IAT Level I cybersecurity baseline certification in accordance with NSA IAD DOC-042-12. **(T-0)**

3.2.13.2.1. No other Communications Security Office role has a mandatory certification requirement.

3.2.13.2.2. Assigned military personnel in an AFSC with a minimum AFSC cybersecurity certification requirement will still meet the AFSC's mandatory certification requirements. **(T-1)**

3.2.13.3. The remaining WCO staff will obtain and maintain, at a minimum, an IAM Level I DoD approved cybersecurity baseline certification. **(T-1)**

3.3. Primary, Additional, and Embedded Duty. In addition to identifying the category and level for each cybersecurity workforce position, these positions must be annotated as a primary, additional, or embedded duty for civilian or military position in accordance with DoD 8570.01-M, Paragraph C7.1.4. **(T-0).** Contractor requirements must be annotated in the contract and associated statement of work or performance work statement if cybersecurity tasks are required. **(T-1)**

3.3.1. Primary Duty. A cybersecurity position with primary tasks focused on cybersecurity tasks. The position may have other tasks assigned, but the main effort focuses on cybersecurity tasks. On average, the position requires at least 25 hours weekly devoted to cybersecurity tasks.

3.3.2. Additional Duty. A position requiring a significant portion of the incumbent‘s attention and energies to be focused on cybersecurity tasks, but in which cybersecurity tasks are not the primary responsibility. On average, the position performs 15 to 24 hours weekly devoted to cybersecurity tasks.

3.3.3. Embedded Duty. A position with cybersecurity tasks identified as an integral part of other major assigned tasks. On average, the position performs up to 14 hours weekly devoted to cybersecurity related tasks.

3.4. Recording the Cybersecurity Workforce Position Requirement. The cybersecurity workforce certification requirements (e.g., category or specialty, certification level, background or security clearance investigation) must be recorded in accordance with DoD 8570.01-M, Paragraph C7.3. **(T-0).** The following paragraphs explain responsibilities within the AF for recording cybersecurity workforce requirements:

3.4.1. Civilian Position. Cybersecurity certification requirements must be recorded in the core personnel document or position description, on the UMD, and within the civilian personnel database(s) or system(s) (e.g., DCPDS). **(T-0)**

3.4.1.1. The PMOs or units must submit a signed personnel action request (e.g., ACR) to the servicing manpower organization for action. **(T-3).** ACR is a tool used to propose changes to the organization, PMO, or unit manpower requirements on the UMD. Please check with servicing manpower organization for ACR template and instructions. At a minimum, the following information must be provided on the personnel action requests: Personnel Accounting Symbol Code (PAS CODE); SEI; Manpower Position Control Number; Civilian Position Control Number; cybersecurity category; cybersecurity level; identification of whether it is a primary, additional, or embedded duty; and an "Information Security [INFOSEC]" annotation as the position specialty. **(T-1)**

3.4.1.2. The PMOs or units must use SEIs to record cybersecurity training and experience requirements on the UMD. **(T-1).** SEIs are used to identify and track unique training and required expertise for a UMD position. If a civilian position is coded with an equivalent enlisted AFSC on the UMD, then the PMO or unit must use the SEIs listed in **Table 3.1** to identify and track cybersecurity training and experience requirements. **(T-1).** Likewise, if a civilian position is coded with an equivalent officer AFSC on the UMD, the PMO or unit must use the SEIs listed in **Table 3.2** **(T-1)**

Table 3.1. Civilian SEIs (Positions Coded with Equivalent Enlisted Air Force Specialty Codes).

Certification Category or Specialty and Level	Civilian SEIs for Positions Coded with an Enlisted AF Specialty Code
IAT Level I	260
IAT Level II	264
IAT Level III	265
IAM Level I	266
IAM Level II	267
IAM Level III	268
IASAE Level I	402
IASAE Level II	403
IASAE Level III	404
CSSP Analyst	872

CSSP Infrastructure Support	873
CSSP Incident Responder	874
CSSP Auditor	875
CSSP Manager	876

Table 3.2. Civilian SEIs (Positions Coded with Equivalent Officer AFSCs).

Certification Category or Specialty and Level	Communications/Computer Systems SEIs **See NOTE**	Operations SEIs **See NOTE**
IAT Level I	C61	O61
IAT Level II	C62	O62
IAT Level III	C63	O63
IAM Level I	C0I	O0I
IAM Level II	C0J	O0J
IAM Level III	C0K	O0K
IASAE Level I	CO1	OO1
IASAE Level II	CO2	OO2
IASAE Level III	CO3	OO3
CSSP Analyst	CO4	OO4
CSSP Auditor	CO5	OO5
CSSP Incident Responder	CO6	OO6
CSSP Infrastructure Support	CO7	OO7
CSSP Manager	CO8	OO8
***NOTE: SEI Activity Code Prefix Definitions**		

C (Computer Systems)	Identifies those civilians who are associated with research, design, development, application, modification, protection, or security of computer systems, networks, or software.
O (Operations)	Identifies civilians directly involved in the employment of cyberspace weapon system(s) to accomplish an operational mission. The operations activity code will also apply to officers serving in staff or commander positions associated with the cyberspace weapon system employment and operational mission accomplishment.

3.4.1.3. PMOs or units must coordinate core personnel document or position description changes with the servicing personnel function (Force Support Squadron or equivalent), servicing Civilian Personnel Section (including the Labor Relations Officer), and civilian classification, in accordance with local processes. **(T-1)**

3.4.1.4. PMOs or units must submit a signed personnel action request (e.g., ACR) to the servicing civilian personnel section for further action by civilian classification to update the civilian personnel database(s) or system(s) (e.g., DCPDS). **(T-1).** At a minimum, the following information must be provided on the personnel action requests: Personnel Accounting Symbol Code; SEI; Manpower Position Control Number; Civilian Position Control Number; cybersecurity category; cybersecurity level; identification of whether it is a primary, additional, or embedded duty; and an “INFOSEC” annotation as the position specialty. **(T-1)**

3.4.2. Military. Cybersecurity position certification requirements are currently recorded in manpower databases or systems (e.g., Manpower Programming and Execution System). This is done through the use of SEIs for officer and enlisted requirements. PMOs or units must use the SEIs listed on **Table 3.3 and Table 3.4** for all military personnel, regardless of AFSC. **(T-1)**

3.4.2.1. The PMO or unit must submit a personnel or manpower change request (e.g., ACR) to the servicing personnel function (Force Support Squadron or equivalent) to include Manpower Position Control Number and valid SEIs. **(T-1)**

3.4.2.2. The AFECD has the current list of enlisted SEIs, and the AFOCD includes the current list of activity codes, Both documents are located on the myPers portal: **https://mypers.af.mil/app/login/redirect/home/session/L3RpbWUvMTU3NzcxNzQ1Ni9nZW4vMTU3NzcxNzQ1Ni9zaWQvZlU1b3RfNVdOeDRKbEg0b0wlN0VXSiU3RUdQb2x6M0EyTzZBdjRGblc1NXl4MzRsSlN2SHI4bTc0UXphVlI0dzklN0VuZzJ4SGp5YVR4S0xNRHdoX1AwcjRDSGxja3RFQThDSkdLZXZQJTdFRVdWV0d1ODkwamdLS2tBQmowNEElMjElMjE=**

3.4.2.3. Do not replace existing SEIs.

Table 3.3. Enlisted SEIs.

Certification Category or Specialty and Level	Enlisted SEIs
IAT Level I	260
IAT Level II	264
IAT Level III	265
IAM Level I	266
IAM Level II	267
IAM Level III	268
IASAE Level I	402
IASAE Level II	403
IASAE Level III	404
CSSP Analyst	872
CSSP Infrastructure Support	873
CSSP Incident Responder	874
CSSP Auditor	875
CSSP Manager	876

Table 3.4. Officer SEIs.

Certification Category or Specialty and Level	Communications/Computer Systems SEIs **See NOTE**	Operations SEIs **See NOTE**
IAT Level I	C61	O61
IAT Level II	C62	O62
IAT Level III	C63	O63
IAM Level I	C0I	O0I
IAM Level II	C0J	O0J
IAM Level III	C0K	O0K
IASAE Level I	CO1	OO1
IASAE Level II	CO2	OO2
IASAE Level III	CO3	OO3
CSSP Analyst	CO4	OO4
CSSP Auditor	CO5	OO5
CSSP Incident Responder	CO6	OO6
CSSP Infrastructure Support	CO7	OO7
CSSP Manager	CO8	OO8
NOTE: SEI Activity Code Prefix Definitions		
C (Computer Systems)	**Identifies those officers who are associated with research, design, development, application, modification, protection, or security of computer systems, networks, or software.**	
O (Operations)	**Identifies officers directly involved in the employment of cyberspace weapon system(s) to accomplish an operational mission. The operations activity code will also apply to officers serving in staff or commander positions associated with the**	

	cyberspace weapon system employment and operational mission accomplishment.

3.4.3. Contractors. The PMOs or unit will ensure contractor cybersecurity requirements (e.g., cybersecurity certifications, clearances, computing environment or operating system training completion certificates, etc.) are specified in the contract (new, renewed, or modified). **(T-0)**

3.4.4. For contractors, the AF 8570 Program will not fund cybersecurity certification training, maintenance fees, or exam vouchers. **(T-1)**

3.5. Deployments and Unit Type Code (UTC).

3.5.1. The UTC responsible command and pilot unit must indicate cybersecurity requirements and SEI. **(T-1)**

3.5.2. Deployment line remarks may be established for each category and level of cybersecurity certification to allow the combatant commanders the flexibility to identify the appropriate cybersecurity workforce requirements in a deployed environment not already identified in the UTC Manpower Details section.

3.5.3. Each military member assigned or tasked as a UTC substitute, where the Mission Capability Statement includes cybersecurity responsibilities, will meet the cybersecurity certification requirements. **(T-1)**

Chapter 4

WORKFORCE QUALIFICATIONS

4.1. Qualified Cybersecurity Workforce Criteria. "Qualified" status is achieved when an individual has fulfilled all of the requirements for their respective category or specialty and level in accordance with DoD 8570.01-M Table AP3.T1. SAF/CN will provide criteria and reporting instructions for each category or specialty and level. The PMOs or units must adhere to the specified criteria for "qualified" designation. **(T-1).** Depending upon workforce category or specialty, qualification criteria may include, but is not limited to, the following items:

4.1.1. Possess a DoD approved cybersecurity baseline certification, in good standing. For military, possess appropriate SEI listed in **Table 3.3** or **Table 3.4**. Specific SEI award criteria is found in the AFECD or AFOCD.

4.1.2. Possess signed formal statement of responsibilities.

4.1.3. Possess a signed privileged statement, if applicable.

4.1.4. Possess additional DoD approved cybersecurity baseline certification, in good standing if applicable.

4.1.5. Possess appropriate and current national security investigation (e.g., Tier 1, Tier 4, etc.) commensurate with assigned tasks.

4.1.6. Possess computing environment or operating system training completion certificate(s) on all operating systems or security-related tool(s) or devices supported by individual's PMO or unit, if applicable.

4.1.7. Complete an On-the-Job Evaluation, if applicable.

4.2. Computing Environment or Operating System Training Completion Requirement. All military, civilians, and contractor personnel possessing (1) an IAT certification or (2) a CSSP (except for the CSSP -Manager position) certification, will complete training (e.g., formal, computer based training, web-based, classroom instruction, on-the-job training, etc.) on the operating system security device, service, or tool that the PMO and unit supports. **(T-0).** The PMOs or units have the flexibility to decide what training, including content and length, is adequate to meet this requirement. The PMO or unit must document individual's successful completion of training. **(T-1).** At minimum, PMO or unit must include the name of individual trained, title of training completed, and date training was completed in documentation. **(T-1)**

4.2.1. The documentation can be stored digitally or electronically or in paper format. The PMO or unit must ensure the documentation is readily accessible, especially during audits or inspections. **(T-1)**

4.2.2. Examples of acceptable documentation include digital or printed certificates, sanitized (i.e., all personally identifiable information, except for name of individual are redacted) copy of transcript, training records, or a memo for record annotating training completion signed by individual's supervisor. **(T-3)**

4.3. Privileged User Agreement . In accordance with DoD 8570.01-M, Paragraph C2.1.4 and Table AP3.T1, all individuals (military, civilians, and contractors) who are required to possess an IAT (Level I, Level II, and Level III) or in the CSSP Specialty (except for CSSP Manager) certifications will complete and sign a Privileged User Agreement. **(T-0)**

4.3.1. The individual will sign the Privileged User Agreement, stating position or role responsibilities, prior to gaining access to Information System, network, or PIT System. (T-0). Digital signatures are acceptable.

4.3.2. The WCO will maintain a copy of the signed Privileged User Agreement. (T-3)

4.4. Additional Cybersecurity Certification Requirement. Those individuals assigned to CSSP positions will achieve additional cybersecurity certification as described in **Paragraph 3.2.7** and its subparagraphs. **(T-0)**

Chapter 5

CYBERSECURITY WORKFORCE CERTIFICATION PROCESS

5.1. Cybersecurity Baseline Certifications.

5.1.1. Civilian and military assigned to a cybersecurity workforce position will possess and maintain in good standing the DoD approved cybersecurity baseline certification(s) in accordance with DoD 8570.01-M, Paragraph C2.3.7. **(T-0)**

5.1.2. Contractor personnel performing one or more cybersecurity tasks in accordance with contract requirements and associated statement of work or performance work statement will possess and maintain in good standing the DoD approved cybersecurity baseline certification(s) in accordance with DoD 8570.01-M, Paragraph C2.3.7. **(T-0).** Contractors will be certified no later than the first day of contract work in accordance with DoD 8570.01-M, Paragraph C2.3.9. **(T-0)**

5.1.3. Cybersecurity certifications without a continuing education component do not meet the requirements of DoD 8570.01-M.

5.2. Air Force Preferred Cybersecurity Baseline Certifications (Civilian and Military Only).

5.2.1. The AF has developed a preferred list of cybersecurity certifications, based upon the DoD approved cybersecurity baseline certifications. In consultation with AF subject matter experts, AF/A2/6 and SAF/CN staffs will review the AF Preferred List and make changes, as necessary, to meet mission requirements. Those certifications on the AF Preferred List have priority for funding. Contact SAF/CN for more details.

5.2.2. Even though AF has the AF Preferred List, personnel can obtain or maintain certification from the DoD approved cybersecurity baseline certification list that is category or specialty and level specified for the assigned position.

5.3. Minimum Cybersecurity Baseline Certification Requirement. Multiple military AFSCs mandate the possession of minimum cybersecurity certification as a precondition as defined in the AFECD or AFOCD. Refer to the latest AFECD or AFOCD version for requirement details.

5.3.1. A higher level or different category or specialty certification than mandated by AFSC may be required for assigned position.

5.3.2. Exam. The AF 8570 Program will pay for one (1) exam voucher at the specified AFSC requirement unless member occupies an assigned position with different or higher cybersecurity requirements. **(T-1).** The AF 8570 Program will pay for additional exam voucher(s) from the AF Preferred List when individual is assigned to a cybersecurity coded position requiring a higher level certification requirement, certification in a new category or specialty, or multiple DoD approved cybersecurity baseline certifications. **(T-1)**

5.3.3. Maintenance. Civilian and military personnel will comply with **Paragraph 5.8** **(T-1)**

5.3.4. Military personnel in AFSCs with a minimum 8570 cybersecurity certification requirement will maintain the highest level baseline certification obtained in good standing, to meet AFSC requirement, even while serving in a joint or special duty assignment. **(T-1)**

5.3.5. Chief Master Sergeants or Senior Master Sergeants. Cybersecurity certifications are not mandatory for Chief Master Sergeants or Senior Master Sergeants, except for those members assigned to cybersecurity-coded positions. The AF 8570 Program will pay certification maintenance fees for those individuals already possessing a DoD-approved certification off the AF Preferred List. **(T-1).** The AF 8570 Program will not provide exam vouchers for new certifications for Chief Master Sergeants and Senior Master Sergeants unless filling a cybersecurity-coded position. **(T-1)**

5.4. Support for the Cyber Operations Career Field (17XX). Graduates of Undergraduate Cyber Training will continue to obtain IAM Level I DoD approved cybersecurity baseline certification as a precondition for matriculation into the career field. **(T-1)**

5.4.1. If assigned to cybersecurity-coded position, Cyber Operations (17XX) officers will obtain required DoD approved cybersecurity baseline certification within six (6) months of duty assignment. **(T-1)**

5.4.2. Exam. The AF 8570 Program will pay for one (1) exam voucher at the specified AFSC requirement unless member occupies an assigned position with different or higher cybersecurity requirements. **(T-1).** The AF 8570 Program will pay for additional exam voucher(s) from the AF Preferred List when individual is assigned to a cybersecurity coded position requiring a higher level certification requirement, certification in a new category or specialty, or multiple DoD approved cybersecurity baseline certifications. **(T-1)**

5.4.3. Once a DoD approved cybersecurity baseline certification is obtained, 17X officers will maintain their baseline certification in good standing, even while serving in a joint assignment, special duty assignment or deployment. **(T-1)**

5.5. Exams (Civilians and Military Only). The certification exam voucher is used to pay for a certification exam. Vouchers may be requested via this Air Combat Command Cyberspace Support Squadron link: **https://cyss.us.af.mil/cyss/certifiedworkforce**.

5.5.1. The AF 8570 Program will pay for one (1) DoD approved cybersecurity baseline certification exam to meet the category and level of the cybersecurity-coded position or AFSC requirement. **(T-1).** The AF 8570 Program will pay for an additional exam voucher(s) when an individual is assigned to a cybersecurity-coded position requiring multiple DoD approved cybersecurity baseline certifications. **(T-1).** Those certifications on the AF Preferred List have priority for funding. An individual can request an exam voucher for a higher level DoD approved cybersecurity baseline certification within the same category or specialty.

5.5.1.1. : Retirement or Separation Restriction: The AF 8570 Program will not be used to pay for an exam voucher for civilian and military personnel who are within one (1) year of a confirmed retirement or separation date. **(T-1)**

5.6. Certification Exam Failure or Decertification. This section applies to every military member who fails DoD approved cybersecurity baseline certification exams or does not possess the required DoD approved cybersecurity baseline within six months of assignment of tasks. Likewise, this section applies to civilians who do not possess the required DoD approved cybersecurity baseline within six months of assignment of tasks. Furthermore, this section applies to civilians, military, and contractors who become decertified (please see **Paragraph 5.6.6**). Civilian and military personnel may be subject to administrative action if they do not obtain or maintain baseline certifications.

5.6.1. Except for re-testing conducted at initial skills training (IST) or schoolhouses, the AF 8570 Program will not pay for any re-testing required after an initial exam failure or decertification for civilians or military. **(T-1).** The individual will be responsible for paying to re-test. **(T-1).** The PMOs or units may fund with internal resources for a re-testing. In coordination with AF/A2/6, SAF/CN may make exceptions on a case-by-case basis.

5.6.2. Military, civilian, and contractor personnel who fail to maintain active (i.e., in good standing) certification(s) will not be allowed an unsupervised privileged account in accordance with DoD 8570.01-M, Paragraph C3.2.4.6. **(T-0)**

5.6.3. Civilian Personnel. If a civilian has not obtained a DoD approved cybersecurity baseline certification commensurate to category and level of the assigned position within six months of assignment, then the civilian will not perform any assigned cybersecurity tasks unless under the direct supervision of a cybersecurity certified individual. **(T-1).** The commander determines appropriate actions, in accordance with local civilian personnel policies, based on the type of cybersecurity position held as follows:

5.6.3.1. Primary Duty. The commander will immediately contact the servicing civilian personnel section and local administrative procedures will be followed. **(T-3)**

5.6.3.2. Additional Duty. Those additional tasks (cybersecurity) must be reassigned to another individual who has the appropriate certification in good standing. **(T-1).** The commander will have the discretion to allow individuals to resume additional tasks, once baseline certification is obtained. **(T-3)**

5.6.3.3. Embedded Duty. Those embedded tasks (cybersecurity) must be reassigned to another individual who has the appropriate certification in good standing. **(T-1).** The commander will have the discretion to allow individuals to resume embedded tasks, once baseline certification is achieved. **(T-1)**

5.6.4. Military Personnel. Military personnel who fail their initial DoD approved cybersecurity baseline certification exam may be placed in remedial supervised training (e.g., computer based training [CBT], hands-on training, or instructor-led training). If a military member has not obtained a DoD approved cybersecurity baseline certification commensurate to category and level of assigned position within six months of assignment, then the commanders of PMOs or units will reassign cybersecurity tasks to another individual who has the appropriate certification in good standing. **(T-1).** Commanders will adhere to **Attachment 3** for the Military Certification Failure Matrix. **(T-1)**

5.6.4.1. The commander should meet with both the supervisor and military member to reassess whether the individual possesses the necessary skills to perform in a cybersecurity position. This assessment should include, but is not limited to, an individual's aptitude, motivation, experience, and knowledge level to perform in a cybersecurity position.

5.6.4.2. Initial Certification. Where obtaining a DoD approved cybersecurity baseline certification is a requirement for matriculation (i.e., entry) into an AFSC, commanders will begin AFSC disqualification actions in accordance with AFI 36-2101, *Classifying Military Personnel (Officer and Enlisted),* after second test failure **(T-1).** Otherwise, commanders of PMOs or units have the discretion to retain the individual or pursue other appropriate administrative actions.

5.6.4.3. If the military member is retained, supervisors should validate the member's readiness for re-testing and ensure the person is scheduled to retake the certification.

5.6.5. Contractors. Contractor personnel will meet certification requirements as outlined in their contract requirements and will not be assigned to nor will not perform any cybersecurity tasks in which they are not certified in accordance with DoD 8570.01-M, Paragraph C2.3.9. **(T-0).** Timelines for contractor software developers, engineers, or programmers to be certified are noted in **Paragraph 3.2.12.2**. Any issues concerning contract requirements (e.g., cybersecurity certification requirements) should be addressed through the Contracting Officer.

5.6.6. Decertification: Decertification includes those individuals whose certifications are expired, terminated, or withdrawn by issuing commercial certification provider for any reason (e.g., failure to meet CEU or CPE standards, failure to pay maintenance fees, etc.). Decertification equates to an "exam failure." If decertification occurs, the commander of the PMO or unit takes the following action, depending on the status of the individual:

5.6.6.1. Military. The commander of PMO or unit has the discretion to retain the individual or pursue other appropriate administrative actions. If required certification is not maintained for any reason, applicable SEI code must be removed from individual's military personnel records. **(T-1)**

5.6.6.2. Civilian. The commander of PMO or unit determine the appropriate action(s) in accordance with local civilian personnel policies if civilian has not maintained requisite DoD approved cybersecurity baseline certification(s). The commander may allow up to six (6) months additional time for recertification. However, the commander of PMO or unit will reassign cybersecurity tasks to another individual who has the appropriate certification in good standing until recertification is achieved. **(T-1)**

5.6.6.3. Contractor. If contractor employee has not obtained or has not maintained required DoD approved cybersecurity baseline certification(s)**,** Contracting Officer will immediately notify contract prime company to stop contractor employee from performing any cybersecurity-related work on a government contract with cybersecurity requirements. **(T-0)**

5.7. Continuing Education Units (CEUs) or Continuing Professional Education (CPE). DoD approved cybersecurity baseline certifications require CEUs or CPEs to stay current. Commercial certification providers define the criteria for acceptable CEUs or CPEs. All certification holders (military, civilians, and contractors) will adhere to CEU or CPE policies set by their respective certification provider(s) in accordance with DoD 8570.01-M, Paragraph 2.3.1 and Table AP3.T1. **(T-0).** Some commercial certification providers may allow CEUs or CPEs for work experience that is documented and verified. Also, CBTs may count toward CEUs or CPEs (please check with the commercial certification provider for details) and are available via various DoD resources (e.g., AF e-Learning program for civilians and military).

5.8. Maintenance of Cybersecurity Baseline Certifications.

5.8.1. Civilian, military, and contractor personnel will maintain the highest-level DoD approved cybersecurity baseline certification obtained for category or specialty as required by UMD position, AFSC, or contract requirements. **(T-1)**

5.8.2. For civilian and military personnel, the AF 8570 Program will pay, as funding requirement priority, the maintenance fees for DoD approved cybersecurity baseline certification(s) on the AF Preferred List only for individuals required by assigned position requirements, mandated by AFSC, or for civilians who already possess baseline certification(s) and occupy a career-broadening position. **(T-1).** See **Paragraph 5.2** for details on the AF Preferred List process. The maintenance fee vouchers may be requested via this Air Combat Command Cyberspace Support Squadron link: **https://cyss.us.af.mil/cyss/certifiedworkforce**.

5.8.2.1. For civilian and military personnel, the AF 8570 Program will pay maintenance fees for the highest level certification on the AD Preferred List necessary to meet category or specialty requirements of assigned position or AFSC. **(T-1)**

5.8.2.2. The AF 8570 Program will pay maintenance fees only for certifications on the AF Preferred List, enabling eligible civilian and military personnel to remain in good standing up to and including effective retirement or separation date. **(T-1)**

5.8.2.3. The AF 8570 Program will pay maintenance fees for multiple DoD approved cybersecurity baseline certifications on the AF Preferred List, if the civilian or military member is assigned to a cybersecurity workforce position, requiring multiple certifications. **(T-1)**

5.8.3. The AF 8570 Program does not pay maintenance fees for contractors in accordance with **Paragraph 3.4.4**.

5.8.4. Civilian, military, and contractor personnel will authorize a new certification release, whenever a certification is issued or renewed, to DoD in accordance with DoD 8570.01-M, Paragraph C2.3.12. **(T-0).** Personnel can access and submit release authorization at this link: **https://cyss.us.af.mil/cyss/certifiedworkforce/**.

5.9. Recording Certification Completion. In addition to authorizing release the certification information status to DoD, additional actions to record certification completion are the following for civilians and military:

5.9.1. Civilian. Civilian personnel can update civilian personnel database(s) or system(s) through a self-certification process in the MyBiz+ application. The status of the certification would be listed as "self-certified" in the member's record. The member should then receive an automated email with a link to upload the certificate into the AF Personnel Services application where it is verified by AF Personnel Center at Joint Base San Antonio -Randolph, TX. Once verified, the status in MyBiz+ would change to “Verified.” Until the member uploads a copy of the certification in AF Personnel Services, the member would remain in an uncertified status for reporting purposes. MyBiz+ is available on the DCPDS portal: **https://compo.dcpds.cpms.osd.mil/**.

5.9.2. Military. Military personnel (officers and enlisted) will complete AF Form 2096, *Classification/On-the-Job Training Action*, to indicate award of the SEI for the highest cybersecurity certification obtained. **(T-1)**

5.9.2.1. The SEI should reflect coding for assigned UMD billet or position or AFSC certification requirement.

5.9.2.2. The AF Form 2096 should be submitted no later than 10 duty days after the effective date of completing the DoD approved cybersecurity baseline certification. Once the supervisor and commander sign the Form, the Form 2096 should be submitted to the appropriate servicing personnel function (e.g., Force Support Squadron, Military Personnel FPF, or equivalent) to update member's personnel record.

5.10. Recording Computing Environment or Operating System Training Completion. A computing environment or operating system training completion certificate must be awarded to meet computing environment or operating system training requirement in accordance with DoD 8570.01-M, Table AP3.T1. **(T-0).** Completion certificates must be maintained locally. **(T-3)**

5.11. Community College of the Air Force Credit. An individual's cybersecurity certification may be accepted for credit at the Community College of the AF, as applicable based on the degree requirements. Individuals should contact their local education office to verify applicability.

Chapter 6

CYBERSECURITY WORKFORCE TRAINING

6.1. Initial Skills Training . Initial skills training (IST) for various AFSCs include cybersecurity concepts and practices as well as an organic, school-house provided test preparation course for cybersecurity certification exam. For those civilian and military personnel who both cannot attend one of these IST programs, distributive or online learning is available, or units can select to fund training.

6.2. Training Resources. Distributive learning resources are available at no cost to civilian and military users via E-Learning on the AF Portal. Another distributive learning resource is the Federal Virtual Training Environment, managed by the Department of Homeland Security. PMOs or units have the discretion to provide additional training resources that can supplement resources provided by AF/A2/6, SAF/CN, or Air Combat Command Cyberspace Support Squadron.

6.3. Authorizing Official Training. The Authorizing Official will obtain training through the DoD Authorizing Official Course. **(T-0).** Authorizing Official training can be found on the DoD Cyber Exchange NIPR portal: **https://cyber.mil/training/dod-authorizing-official-ao/**.

6.4. Contracted Training. PMOs or units may acquire, with their own funds, instructor-led training and virtual instructor-led training to provide certification specific training for personnel unable to obtain certification through distributive learning. The PMO or unit should use appropriate contracting methods.

6.5. Military Computing Environment or Operating System Training Options.

6.5.1. AF Specialty training schoolhouses or technical schools are the foundation for military cyber training and provide apprentice-level qualification.

6.5.2. CBTs or DoD developed classroom training should be leveraged to provide additional Computing Environment or Operating System training not covered by formal AF Specialty training, schoolhouse technical schools, or commercially available courses.

6.5.3. Computing Environment or Operating System training completion certificates can be obtained from vendor-provided commercial training. However, commercial training is at the discretion of and can be funded by the MAJCOM or individual PMO or unit. The PMO or unit should use appropriate contracting methods.

6.6. Civilian Computing Environment or Operating System Training Options.

6.6.1. Use of CBTs or DoD developed classroom training are the preferred methods for obtaining Computing Environment or Operating System training completion certificates. Training can be obtained through various sources (e.g., AF learning management system, the DoD Cyber Exchange NIPR portal, etc.).

6.6.2. Computing Environment or Operating System training completion certificates may be obtained from commercial sources. However, this training is at the discretion of and can be funded by the MAJCOM or individual PMO or unit. The PMO or unit should use appropriate contracting methods.

6.7. Contractor Computing Environment or Operating System Training Options. Contractors will be responsible for their own Computing Environment or Operating System training, unless otherwise stated in the contract requirements**. (T-3)**

Chapter 7

CYBERSECURITY BASELINE CERTIFICATION WAIVERS (CIVILIANS AND MILTARY ONLY)

7.1. In accordance with DoD 8570. 01-M, Paragraphs C3.2.4.2, C3.2.4.3, C4.2.3.2.1, and C4.2.3.2.2, the Authorizing Official has the authority to suspend temporarily via waivers the DoD approved cybersecurity baseline certification requirements for civilian and military personnel due to severe operational or personnel constraint cases. This waiver authority is only applicable to the Information System or PIT System under the Authorizing Official's responsibility. This waiver authority is not applicable to military personnel to meet an AFSC minimum 8570 cybersecurity certification requirement. The waivers must not be authorized for contractor personnel in accordance with DoD 8570.01-M, Paragraphs C3.2.4.1.1, C4.2.3.2, and C11.2.4.1.1. **(T-0)**

7.2. Waiver Process. The waiver must comply with following steps:

7.2.1. The waiver must be documented, preferably in memorandum for record format. **(T-0)**

7.2.2. The waiver must include justifications or reason(s) for waiver. **(T-0).** Reasons should be mission-related.

7.2.3. The waiver must state an expiration date and must not exceed more than six (6) months except for deployment. **(T-0).**

7.2.4. The waiver must state when the certification should be accomplished. **(T-0)**

7.2.5. Consecutive waivers must not be authorized except for deployments to areas declared hostile **(T-0).** For personnel deployed to areas declared hostile, the Authorizing Official has the authority to issue a waiver with an expiration not to exceed more than 6 months after deployment return in accordance with DoD 8570.01-M, Paragraphs C3.2.4.3, C4.2.3.4.2, C10.2.3.4.2, and C11.2.4.3.

7.2.6. A copy of the signed waiver must be inserted in the individual's training record. **(T-1)**

7.2.7. The PMO or unit must forward a copy of the Authorizing Official-signed waivers to the AF Chief Information Security Officer or Chief Information Security Officer's designated representative. **(T-1)**

7.2.8. Certification waivers must be tracked locally. **(T-3)**

7.2.9. Consecutive waivers are not authorized. **(T-0)**

WILLIAM E. MARION II, SES, DAF
Deputy Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 112-239, *National Defense Authorization Act for Fiscal Year 2013*

Committee on National Security Systems Instruction 4009, *Committee on National Security Systems Glossary*, 6 April 2015

DoD Directive 8140.01 Change 1, *Cyberspace Workforce Management*, 31 July 2017

DoD Instruction (DoDI) 8530.01 Change 1, *Cybersecurity Activities Support to DoD Information Network Operations*, 25 July 2017

DoD 8570.01-M Change 4, *Information Assurance Workforce Improvement Program*, 10 November 2015

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 17-2, *Cyberspace Operations*, 12 April 2016

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 23 January 2020

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 36-205, *Affirmative Employment Programs, Special Emphasis Programs, and Reasonable Accommodation Policy*, 1 December 2016

AFI 36-2101, *Classifying Military Personnel (Officer and Enlisted)*, 25 June 2013

AFI 38-206, *Additional Duty Management*, 10 July 2018

Methods and Procedures Technical Order 00-33A-1202, *Air Force Network Account Management*, 18 March 2014

National Security Agency Information Assurance Directorate (NSA IAD) DOC-042-12, *Process Security Doctrine for the Enrollment of Key Management Infrastructure (KMI) Managers*, July 2012

Adopted Forms

DD Form 2875, *System Authorization Access Request [SAAR]*, August 2009

AF Form 847, *Recommendation for Change of Publication,* 22 Sep 2009

AF Form 2096, *Classification/On-the-Job Training Action*, 3 October 2017

Prescribed Forms

None

Abbreviations and Acronyms

AF—Air Force

AF CISO—AF Chief Information Security Officer

AFECD—Air Force Enlisted Classification Directory

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAN—Air Force Manual

AFNET—AF Network

AFNET-S — AF Network—Secure

AFOCD—Air Force Officer Classification Directory

AFPD—Air Force Policy Directive (AFPD)

AFSC—Air Force Specialty Code

AODR—Authorizing Official Designated Representative

CBT—Computer Based Training

CEU—Continuing Education Unit

CIO—Chief Information Officer

CPE—Continuing Professional Education

CSSP—Cyber Security Service Provider

CSSP-A—Cyber Security Service Provider Analyst

CSSP-AU—Cyber Security Service Provider Auditor

CSSP-IR—Cyber Security Service Provider Incident Responder

CSSP-IS—Cyber Security Service Provider Infrastructure Support

DCPDS—Defense Civilian Personnel Data System

DoD—Department of Defense

DoD CIO—DoD Chief Information Officer

DoDD—Department of Defense Directive

DoDIN—DoD Information Network

IA—Information Assurance

IAM—Information Assurance Management Category

IASAE—Information Assurance System Architects and Engineers

IAT—Information Assurance Technical Category

INFOSEC—"Information Security" (The parenthetical title in DCPDS for Civilian personnel performing security [cybersecurity] tasks)

ISSO—Information System Security Officer

ISSM—Information System Security Manager

IT—Information Technology

KMI—Key Management Infrastructure

MAJCOM—Major Command

NIPR—Nonclassified or Nonsecure Internet Protocol Router

NIPRNet—Nonclassified or Nonsecure Internet Protocol Router Network

NSA IAD—National Security Agency Information Assurance Directorate

PIT—Platform Information Technology

PMO—Program Management Office

RMF—Risk Management Framework

SAAR—System Authorization Access Request

SCAR—Security Control Assessor Representative

SEI—Special Experience Identifier

SIPRNet—Secure Internet Protocol Router Network

SME—Subject matter expert

UMD—Unit Manning Document

WCO—Wing Cybersecurity Office

Terms

AF 8570 Program—Is an initiative to certify, manage, and track the AF military and civilian cybersecurity workforce as well as manage and track the contractor cybersecurity workforce.

AF 8570 Program Funds—Refers to the centralized budget or funds managed by Air Combat Command Cyberspace Support Squadron to pay for DoD approved cybersecurity baseline certifications exams and maintenance fees for civilian and military personnel due to AFSC or position-based requirements.

AF Information Network (AFIN)—The globally interconnected, end-to-end set of AF information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to AF warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (Source: AFPD 17-2).

AF Network (AFNET)—The AF's underlying Nonclassified or Nonsecure Internet Protocol Router Network (NIPRNet) that enables AF operational capabilities and lines of business, consisting of physical medium and data transport services. (Source: AFPD 17-2).

AF Network—Secure (AFNET-S) - The AF's underlying Secure Internet Protocol Router Network (SIPRNet) that enables AF operational capabilities and lines of business, consisting of physical medium and data transport services. (Source: AFPD 17-2)

Civilians—AF Government employees paid by appropriated funds or non-appropriated fund (NAF).

Contractor—Private sector employee (US citizen or foreign national) performing an activity or activities in support of contract requirements.

Cybersecurity workforce—All military, civilian, military, and contractors who are performing at least one cybersecurity task in accordance with DoD 8570.01-M.

Cyber Security Service Provider (CSSP)—An organization that provides one or more cybersecurity services to implement and protect the DODIN. Replaces Computer Network Defense – Service Provider.

Foreign National—Individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees, and contractors. (Source: DoD 8570.01-M).

IA Management (IAM)—Refers to the management category of 8570 cybersecurity certification, but is not synonymous with the Information System Security Manager (ISSM) position.

Internet Protocol—The communication protocol for AFNET and AFNET-S. AFNET is a Network Environment example. For this manual, AFNET or AFNET-S is considered as one networking environment, not two.

Major Command (MAJCOM)—The term is synonymous to Field Operating Agency and Direct Reporting Unit for this manual.

Military—Synonymous to the Total Force (Active AF, Air National Guard, and AF Reserve Components).

Networking Environment—Refers to an infrastructure, based upon a communications protocol that governs information exchange among interconnected systems and nodes or stations.

Position—Term is synonymous to a military billet and Government civilian position for this manual.

Privileged User—A user that is authorized to have elevated network rights to perform security-relevant tasks that ordinary users are not authorized to perform. (Source: Committee on National Security Systems Instruction 4009, *Committee on National Security Systems Glossary*)

Program Management Office (PMO)—Manages the acquisition, delivery, and sustainment of information technology, including Information Systems and PIT Systems. Term is synonymous with System Program Office (SPO).

Task—An activity an individual performs on a regular basis to complete assigned job duties. Term is synonymous with function for this manual.

Weapon System—A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (Source: AFPD 17-2).

Attachment 2

AIR FORCE CYBERSECURITY WORKFORCE POSITION CERTIFICATION DETERMINATION GUIDE – TECHNICAL CATEGORY MATRIX

A2.1. Technical Category Matrix. Use the information in Table A2.1, to determine actions commensurate with the role, position, duty description, responsibilities and privileges of assigned personnel. Table A2.1 should be used as a starting point in determining required Cybersecurity workforce position certification levels. Follow additional tables for determination listed in this attachment.

Table A2.1. Technical Category Matrix.

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 1: Backup & restore files, operating system (OS), data, etc. on end-user device(s).	**X**		
Task 2: Check, diagnosis, and repair end-user hardware or software and IT.	**X**		
Task 3: Execute any cyber task or effect using privileged credentials on a local system or end-user device.	**X**		
Task 4: Install, maintain, patch, upgrade local or end-user IT systems or devices (e.g., workstations, printers, multi-function devices, etc.), including operating system software.	**X**		
Task 5: Perform Methods and Procedures Technical Order 00-33A-1202 AFNET user account management tasks	**X**		

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 6: Support, administer, and operate non-standard networked Information System(s) or PIT System(s) (e.g., Internet Protocol managed land mobile radio networks, Voice over Internet Protocol networks, etc.) in Base Area Network or Computing Environment	**X**		
Task 7: Analyze information assurance vulnerability alert (IAVA) and equivalent taskings for mission impact(s) for Base Area Network or Computing Environment		**X**	
Task 8: Analyze, interpret, & develop vulnerability countermeasures for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 9: Check, diagnosis, and repair hardware or software & administer IT systems or Platform Information Technologies (PITs) supporting mission systems (e.g., Command and Control Personal Computer, Global Command & Control System, PMO system that directly connects with an aircraft) in the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 10: Conduct system audits & scans (e.g., Assured Compliance Assessment Solution [ACAS] scans, Automated Remediation and Asset Discovery [ARAD] tasks, System Center Configuration Manager [SCCM] tasks).		**X**	
Task 11: Create, and modify privileged accounts, service accounts, or active directory objects that are servers).		**X**	
Task 12: Develop on-the-job training for IAT Level I and II DoD personnel, support in a Networking Environment (e.g., NIPRNet or SIPRNet)		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 13: Examine vulnerabilities and approve steps to mitigate (e.g., Plan of Action & Milestones [POAMs])		**X**	
Task 14: Examine potential network security or policy breach.		**X**	
Task 15: Execute vulnerability countermeasures (e.g., cyber orders, Information Assurance Vulnerability Management, Time Compliance Network Orders, manual patching, etc.) for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S		**X**	
Task 16: Formulate or provide input into Strategic IT acquisition for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 17: Identify and request Authorized Service Interruption (ASI) that affect two or more sites in the following environments • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 18: Install, maintain, and upgrade servers or network devices (e.g., hubs, gateways, routers, switches).		**X**	
Task 19: Lead unit or teams in support of (ISO) cyber orders & operations (e.g., Mission Defense Team, Defense cyber operations, Service or National Cyber Protect Team leaders) in the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 20: Maintain sensors.		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 21: Manage access & edge layer devices in accordance with guidance and directives from ACC Cyberspace Capabilities Center per AFMAN 17-1301 Ch 2.5 for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 22: Manage role based access control & access control list for systems & devices in the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 23: Manage server side rules and permissions on application-level systems (e.g., SharePoint® , Information Assurance Officer Express Express).		**X**	
Task 24: Perform Methods and Procedures Technical Order 00-33A-1202 AFNET computer account management tasks.		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 25: Plan & deploy sensors (e.g., host & network based IDS) for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 26: Provide subject matter expert support for cyber orders operations & deployment for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 27: Run vulnerability scans.		**X**	
Task 28: Support, administer, and operate non-standard networked IT systems or PITs (e.g., Internet Protocol managed land mobile radio networks, Voice over Internet Protocol networks, etc.) in the following environments: • Networking Environment (e.g., AFNET or AFNET-S) • AFIN		**X**	

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 29: Support, administer, and operate performance or security monitoring systems (e.g., System Center Operations Manager, Manager of Managers, etc.) for the following environments: • Base Area Network or Computing Environment • Networking Environment (e.g., AFNET or AFNET-S)		**X**	
Task 30: Analyze information Assurance vulnerability alert (IAVA) and equivalent taskings for mission impacts			**X**
Task 31: Analyze, interpret, & develop vulnerability countermeasures for the AFIN.			**X**
Task 32: Develop on-the-job training for IAT Level I and II DoD personnel working the AFIN level.			**X**
Task 33: Examine enterprise-wide vulnerabilities and approve steps to mitigate (e.g., POAMs) for the entire AFIN.			**X**

Task	**Information Assurance Technical (IAT) Level I**	**IAT Level II**	**IAT Level III**
Task 34: Execute vulnerability countermeasures (e.g., cyber orders, Information Assurance Vulnerability Management, Time Compliance Network Orders, manual patching, etc.) for the entire AFIN.			**X**
Task 35: Formulate or provide input into Strategic IT acquisition for the AFIN.			**X**
Task 36: Identify and request Authorized Service Interruption (ASI) that affect two or more sites.			**X**
Task 37: Install, maintain, upgrade core service network devices (e.g., Information Transfer Nodes, Service Delivery Point Routers, Primary Domain Controllers, etc.).			**X**
Task 38: Lead unit or teams ISO cyber orders & operations (e.g., Mission Defense Team, Defense cyber operations, Service or National Cyber Protect Team team leaders) for the AFIN.			**X**
Task 39: Manage enclave access & edge layer devices for the entire AFIN in accordance with guidance and directives from ACC Cyberspace Capabilities Center per AFMAN 17-1301 Ch 2.5.			**X**

Task	Information Assurance Technical (IAT) Level I	IAT Level II	IAT Level III
Task 40: Manage role based access control & access control list for systems & devices for the entire AFIN.			**X**
Task 41: Oversee implementation of enterprise-wide (system or application) automation.			**X**
Task 42: Plan & Deploy Sensors (e.g., host & network based IDS) for entire AFIN.			**X**
Task 43: Provide subject matter expert for cyber orders, operations, & deployment for the entire AFIN.			**X**
Task 44: Provide Strategic subject matter expert input for cybersecurity policies, procedures, or standards.			**X**
Task 45: Support, administer, and operate performance or security monitoring systems (e.g., System Center Operations Manager, Manager of Managers, etc.) at the AFIN level.			**X**
Task 46: Troubleshoot hardware or software & administer Information System(s) or PIT System(s), supporting mission systems (e.g., Command and Control Personal Computer, Global Command & Control System, PMO system that directly connects with an aircraft), operating on multiple Networking Environments.			**X**

Table A2.2. Management Category.

Task	Information Assurance Management (IAM) Level I	IAM Level II	IAM Level III
Task 1: Assist in the technical development of cybersecurity assessment and authorization documentation.	**X**		
Task 2: Collect and maintain technical data needed to meet server cybersecurity reporting requirements.	**X**		
Task 3: Develop or modify cybersecurity program plans and requirements for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 4: Develop procedures to ensure system users are aware of their cybersecurity responsibilities before granting access to Information System(s) or PIT System(s).	**X**		
Task 5: Ensure system security configuration guidelines are followed.	**X**		
Task 6: Ensure cybersecurity requirements are appropriately identified for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) only.	**X**		

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 7: Identify a possible security violation and take appropriate action to report the incident, as required.	**X**		
Task 8: Monitor system performance and review for compliance with security and privacy requirements in accordance with AFI 33-332, *Air Force Privacy and Civil Liberties Program*, on client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 9: Supervise or manage implementation of protective or corrective controls or measures when a cybersecurity incident or vulnerability is discovered or reported.	**X**		
Task 10: Use federal and organization specific published documents to manage operations on client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 11: Advise the Authorizing Official of any changes to the cybersecurity posture of an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 12: Assist in the gathering and preservation of evidence used in the prosecution of computer crimes.		**X**	
Task 13: Conduct security assessment and correct security weaknesses on an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 14: Develop cybersecurity requirements for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	

Task	Information Assurance Management (IAM) Level I	IAM Level II	IAM Level III
Task 15: Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		X	
Task 16: Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow cybersecurity policies and procedures for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		X	
Task 17: Ensure that compliance monitoring occurs, and review results of such monitoring of an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		X	

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 18: Ensure that cybersecurity inspections, tests, and reviews are coordinated for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 19: Ensure that software, hardware, and firmware comply with appropriate security configuration guidelines, policies, and procedures for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 20: Ensure recovery processes are monitored and that cybersecurity features and procedures are properly restored for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 21: Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for an Information System or PIT System that operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 22: Evaluate and validate security controls in support of assessment and authorization (formerly called certification and accreditation) activities for final determination by the Authorizing Official.		**X**	
Task 23: Identify alternative cybersecurity strategies for an Information System or PIT System operates in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 24: Monitor contract performance and review deliverables for conformance with contract requirements related to cybersecurity and privacy in accordance with AFI 33-332 for an Information System or PIT System that operates in a Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 25: Oversee the preparation of cybersecurity assessment and authorization documentation for an Information System or PIT System operating in one Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	
Task 26: Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the cybersecurity of an Information System or PIT System in a Networking Environment (e.g., NIPRNet or SIPRNet).		**X**	

Task	Information Assurance Management (IAM) Level I	IAM Level II	IAM Level III
Task 27: Provide leadership and direction to personnel supporting an Information System or PIT System operating in a Networking Environment (e.g., NIPRNet or SIPRNet).		X	
Task 28: Recommend resource allocations required to securely operate and maintain an Information System or PIT System in a Networking Environment (e.g., NIPRNet or SIPRNet).		X	
Task 29: Review security controls and safeguards to determine if security concerns identified in the approved plan have been fully addressed in an Information System or PIT System in one Networking Environment (e.g., NIPRNet or SIPRNet).		X	
Task 30: Support assessment of security controls and conduct initial remediation actions in preparation for system authorization using DoD assessment procedures (e.g., Security Recommendation Guides & Security Technical Implementation Guides).		X	

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 31: Advise the Authorizing Official of changes to the cybersecurity posture for AFIN.			**X**
Task 32: Approve cybersecurity assessment and authorization documentation.			**X**
Task 33: Analyze, develop, approve, and issue cybersecurity policies for the entire AFIN or multiple Networking Environments.			**X**
Task 34: Analyze identified cybersecurity strategies and select the best approach or practice for an Information System or PIT System, operating in multiple Networking Environments.			**X**
Task 35: Develop the Continuity of Operations Plan for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 36: Ensure information ownership responsibilities are established for an Information System or PIT System, operating on multiple Networking Environments.			**X**

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 37: Ensure that protection and detection capabilities are acquired or developed for an Information System or PIT System, operating on multiple Networking Environments.			**X**
Task 38: Ensure that security related provisions of the system acquisition documents meet all identified cybersecurity needs for Information System(s) or PIT System(s) operating on multiple Networking Environments.			**X**
Task 39: Evaluate and approve development efforts to ensure that baseline cybersecurity safeguards are appropriately installed for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 40: Evaluate cost benefit, economic and risk analyses for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 41: Evaluate proposals to determine if proposed cybersecurity solutions effectively address requirements for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 42: Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 43: Identify IT cybersecurity program implications of new technologies or technology upgrades.			**X**
Task 44: Interpret or approve cybersecurity requirements relative to the capabilities of new information technologies.			**X**
Task 45: Interpret patterns of noncompliance to determine their impact on levels of risk or overall effectiveness of cybersecurity program for Information System(s) or PIT System(s), operating in multiple Networking Environments.			**X**

Task	**Information Assurance Management (IAM) Level I**	**IAM Level II**	**IAM Level III**
Task 46: Monitor and evaluate the effectiveness of security posture for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 47: Oversee the preparation of cybersecurity assessment and authorization documentation for Information System(s) or PIT System(s), operating in multiple Networking Environments.			**X**
Task 48: Review security controls and safeguards to determine if security concerns identified in the approved plan have been fully addressed in Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 49: Supervise technical audits or validations of security controls for Information System(s) or PIT System(s), operating in multiple Networking Environments.			**X**
Task 50: Take action as needed to ensure that accepted products or tools meet Common Criteria requirements.			**X**

Table A2.3. IA System Architecture and Engineering (IASAE) Specialty.

Task	**IASAE Level I**	**IASAE Level II**	**IASAE Level III**
Task 1: Assess threats and vulnerabilities only for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 2: Define cybersecurity requirements only for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 3: Design, develop, or implement cybersecurity architecture only for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 4: Design, develop, and implement cybersecurity products and services only for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 5: Design, develop, recommend, and implement countermeasures and mitigations only for client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) vulnerabilities.	**X**		

Task	**IASAE Level I**	**IASAE Level II**	**IASAE Level III**
Task 6: Test and evaluate products and services security and vulnerability countermeasures or mitigations only on client or end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	**X**		
Task 7: Assess threats and vulnerabilities to an Information System or PIT System, operating in one Networking Environment (e.g., NIPRNet or SIPRNet) level.		**X**	
Task 8: Define security requirements for an Information System or PIT System, operating in one Networking Environment (e.g., NIPRNet or SIPRNet) level.		**X**	
Task 9: Design, develop, and implement security architecture for an Information System or PIT System, operating at the Networking Environment (e.g., NIPRNet or SIPRNet) level.		**X**	
Task 10: Design, develop, and implement cybersecurity products and services for an Information System or PIT System, operating at the Networking Environment (e.g., NIPRNet or SIPRNet) level.		**X**	

Task	**IASAE** **Level I**	**IASAE** **Level II**	**IASAE** **Level III**
Task 11: Ensure implementation of cybersecurity policies for an Information System or PIT System, operating only on a Networking Environment (e.g., operating only on NIPRNet or SIPRNet).		**X**	
Task 12: Test and evaluate products and services for security and vulnerability countermeasures or mitigations.		**X**	
Task 13: Assess threats and vulnerabilities to Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 14: Define security requirements for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 15: Design, integrate, test, and evaluate cross-domain solutions.			**X**
Task 16: Design, develop, and implement security architecture for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**

Task	**IASAE Level I**	**IASAE Level II**	**IASAE Level III**
Task 17: Design, develop, and implement security architectures supporting multilevel security requirements (e.g., the processing of multiple classification levels of data UNCLASSIFIED, SECRET, and TOP SECRET).			**X**
Task 18: Design, develop, or implement cybersecurity products and services for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 19: Design, develop, or implement security countermeasures or mitigations to vulnerabilities of Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 20: Develop interface specifications for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**
Task 21: Ensure implementation of cybersecurity policies for Information System(s) or PIT System(s), operating on multiple Networking Environments.			**X**

Task	IASAE Level I	IASAE Level II	IASAE Level III
Task 22: Integrate or implement cross-domain solutions.			X
Task 23: Test and evaluate products and services for security or vulnerability countermeasures and mitigations for Information System(s) or PIT System(s), operating on multiple Networking Environments.			X

Table A2.4. Cybersecurity Service Provider Analyst Position.

Task	Cybersecurity Service Provider Analyst
Task 1: Analyze identified anomalous or malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	X
Task 2: Assist in the development of indicators, alerts, or signatures for cybersecurity tools.	X
Task 3: Correlate cyber events or incidents to information obtaining from sources (e.g., alerts, intelligence, threat reports, etc.) for situational awareness as well as determining the effectiveness.	X
Task 4: Develop reports on cyber events and network traffic.	X
Task 5: Evaluate logs from network resources (e.g., individual host[s), firewalls, intrusion detection, or prevention systems, etc.).	X
Task 6: Evaluate network traffic for anomalous activity or threat indicators.	X
Task 7: Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	X
Task 8: Perform trend analysis and reporting on cyber events or incidents.	X

Table A2.5. Cybersecurity Service Provider Auditor Role.

Task	**Cybersecurity Service Provider - Auditor**
Task 1: Conduct or support authorized penetration testing of network assets.	**X**
Task 2: Perform network vulnerability assessments.	**X**
Task 3: Perform network risk assessments of people, processes, technologies, or operations.	**X**
Task 4: Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies or solutions.	**X**

Table A2.6. Cybersecurity Service Provider Incident Responder Role.

Task	**Cybersecurity Service Provider Incident Responder**
Task 1: Collect and analyze intrusion artifacts (e.g., source code, malware, Trojans, etc.).	**X**
Task 2: Coordinate with intelligence analysts to correlate threat assessment data.	**X**
Task 3: Correlate incident data.	**X**
Task 4: Perform initial, forensically sound collection of images and inspect to discern possible mitigation or remediation.	**X**
Task 5: Perform network trend analysis and reporting.	**X**
Task 6: Perform real-time incident handling (e.g., forensic collections, intrusion correlation or tracking, threat analysis, and direct system remediation) tasks.	**X**
Task 7: Serve as technical experts and liaisons to law enforcement personnel.	**X**
Task 8: Track and document cyber incidents from initial detection through final resolution.	**X**
Task 9: Use discovered data to develop mitigations or remediation to potential network incidents.	**X**
Task 10: Write network guidance and reports on incident findings to appropriate constituencies or stakeholders.	**X**

Table A2.7. Cybersecurity Service Provider Infrastructure Support Role.

Task	Cybersecurity Service Provider Infrastructure Support
Task 1: Configure and manage alerts, indicators, rules, or signatures for cybersecurity applications and tools.	X
Task 2: Create, edit, and manage changes to network access control lists on cybersecurity tools or systems (e.g., firewalls and intrusion prevention systems).	X
Task 3: Implement alerts, indicators, rules, or signatures for cybersecurity applications, systems, and tools.	X
Task 4: Maintain CSSP training lab or network.	X
Task 5: Perform system administration (e.g., install, configure, backup, restore) on cybersecurity applications, systems, and tools.	X
Task 6: Test and evaluate cybersecurity applications systems, tools, rules, signatures, access controls, or configurations of CSSP managed platforms.	X
Task 7: Work with CSSP Analyst(s) to review logs and develop mitigations.	X

Table A2.8. Cyber Security Service Provider Manager Position or Role.

Task	Cybersecurity Service Provider Manager
Task 1: Implement and enforce cybersecurity policies and procedures for Cybersecurity Service Provider, reflecting applicable laws, policies, procedures, and regulations.	X
Task 2: Lead risk analysis and management activities for the network.	X
Task 3: Manage an incident (e.g., coordinate documentation, work efforts, resource utilization) from inception to final remediation and after action reporting.	X
Task 4: Manage monitoring of cybersecurity data sources to maintain situational awareness.	X
Task 5: Manage the publishing of cybersecurity guidance (e.g., Information Assurance Vulnerability Alerts, policies, etc.).	X
Task 16: Manage threat or target analysis of cybersecurity information and production of threat or target information within the network or enclave environment.	X
Task 7: Provide incident reports, summaries, and other situational awareness information to higher headquarters.	X
Task 8: Track compliance audit findings, incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken.	X

Table A2.9. Senior Software Development Positions or Roles.

Task	**Senior Software Development Positions or Roles**
Task 1: Address security implications in the software acceptance phase for the following: completion criteria, risk acceptance & documentation, common criteria, and methods of independent testing.	X
Task 2: Analyze and provide information to stakeholders that would support the development of a security application or modification of an existing security application.	X
Task 3: Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	X
Task 4: Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	X
Task 5: Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	X
Task 6: Define testing criteria for new or updated applications.	X
Task 7: Evaluate factors (e.g., reporting formats required, cost constraints, and need for security restrictions) to determine hardware configuration.	X
Task 8: For major weapon systems, capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	X
Task 9: Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	X
Task 10: Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	X

A2.2. Determination Guide Example Scenarios. See the scenarios below to aid in determinations.

A2.2.1. EXAMPLE SCENARIO 1: Technicians only use elevated permissions when executing yearly patching or hardening efforts for their specific system(s) to include servers and end-user devices. Total time patching is less than two hours. SCENARIO 1 Determination: DoD 8570.01-M, Section AP1.15 states "IA workforce includes anyone with privileged account…" Executing above hardening actions would require the use of elevated permissions or privileges (privileged). Technicians would have to possess at least an approved 8570 IAT Level I cybersecurity certification since described duty would map to this listed IAT Level I duty: Patching end-user device, including operating system

A2.2.2. EXAMPLE SCENARIO 2: Individual administers or manages front-end (web-based interface) SharePoint® site, Information Assurance Officer Express, or other web-based application interface that does NOT require the use of elevated permissions to conduct daily operations. SCENARIO 2 Determination: This task does not involve using elevated permissions or privileges (privileged) to execute actions. No 8570 cybersecurity certification would be required.

A2.2.3. EXAMPLE SCENARIO 3: Individual administers SharePoint® back-end database or other back-end server that provides web-based applications to users. SCENARIO 3 Determination: This task does not require using elevated permissions or privileges (privileged). No 8570 cybersecurity certification would be required.

A2.2.4. EXAMPLE SCENARIO 4: Technicians are responsible for server administration, routers and switches on a radio frequency (RF) network. Some of the equipment uses Internet Protocol connectivity for administration, and the equipment is considered a networked system of devices. SCENARIO 4 Determination: These technicians must have at least an approved 8570 IAT Level II cybersecurity certification because they are responsible for the server, router, or switches.

A2.2.5. EXAMPLE SCENARIO 5: Technicians are conducting network vulnerability scans across end user devices (workstations) at the base level. SCENARIO 5 Determination: Technicians must possess at least an approved 8570 IAT Level I cybersecurity certification.

Attachment 3

MILITARY CERTIFICATION FAILURE POLICY

Table A3.1. Failure Policy Matrix.

Individuals Who Have	**Resulting in**	**Result(s)**	**Responsible Authority**	**Actions(s) Taken**
First cybersecurity certification exam attempt	Passing score	Individual cleared to perform cybersecurity tasks	Supervisor	Assign individual as appropriate
	Failing score	Individual can be placed in remedial, supervised training (CBTs, AF Learning Management System etc.)	Commander and Supervisor	The commander of PMO or unit has the discretion to allow the military member to pursue a second exam attempt or pursue appropriate administrative action(s). If military member's second attempt occurs after six (6) months of assumption of assigned cybersecurity tasks, the commander (PMO or unit) will reassign cybersecurity tasks to another individual who has the appropriate certification in good standing until certification is achieved. Personnel can access and submit release authorization at this link: https://cyss.us.af.mil/cyss/certifiedworkforce/. If "retain and retest": <u>Step 1:</u> The supervisor should document individual's training regimen to include understanding of concepts

				motivation level and study habits. Step 2: Supervisor should validate the individual‘s readiness for retesting. Step 3: Member will not perform any assigned cybersecurity tasks unless under the direct supervision of a cybersecurity certified individual. Due to operational constraints, supervisor or commander could pursue a temporary Authorizing Official approved waiver in accordance within accordance with **Chapter 8**.
Second cybersecurity certification exam attempt	Passing score	Individual is cleared to perform cybersecurity tasks	Supervisor	Assign individual as appropriate
	Failing score	Individual will not perform any cybersecurity tasks, unless under the direct supervision of a cybersecurity certified individual.	Commander and Supervisor	Where obtainment of a DoD approved cybersecurity baseline certification is a requirement for matriculation (i.e. entry) into an AFSC, commanders will begin AFSC disqualification actions in accordance with AFI 36-2101, Paragraph 4.1 after second test failure. Otherwise, the commander (PMO or unit) has the discretion to retain the individual or pursue other appropriate administrative actions(s).

				The commander (PMO or unit) will reassign cybersecurity tasks to another individual who has the appropriate certification in good standing until certification is achieved.

Attachment 4

CYBERSECURITY WORKFORCE METRIC REPORT

A4.1. The cybersecurity workforce metrics report may be completed by using Figure A4,1 as an example as identified in paragraphs 2.7.5, 2.13.2, and 2.14.16.

Figure A4.1. Sample Cybersecurity Workforce Metric example report.

(Appropriate Letterhead)

Date

MEMORANDUM FOR (Individual Concerned)

FROM: ORG/Symbol

SUBJECT: Cybersecurity Workforce Metric report for period xxx

The cybersecurity workforce metrics are provided below in accordance with AFMAN 17-1303:

1. Billets and Positions: By category or specialty (IAT, IAM, IA System Architecture and Engineering (IASAE), and Cyber Security Service Provider [CSSP] Specialty) and level (Level I, II, and III), report the number of authorization.
a. Civilian positions
b. Military billets

2. Assigned Billets and Positions: By category or specialty (IAT, IAM, IASAE, and CSSP) and level (Level I, II, and III), report the number of assigned.
a. Civilian positions
b. Military billets

3. Certified: By category (IAT, IAM, IASAE, and CSSP) and level (Level I, II, and III), report the number of personnel who are in an assigned position, have achieved a DoD approved DoD approved cybersecurity baseline certification for the appropriate category and level, and have released certification data to DoD. Please do not include any individuals with waivers in this total.
a. Civilian
b. Military
c. Contractor

4. Computing Environment or Operating System Training Completion Certificates: This applies mostly to the IAT category and Cyber Security Service Provider (CSSP) Specialty (except for CSSP Manager). By category or specialty (IAT and CSSP) and level (Level I, II, and III), report the number of cybersecurity personnel with privileged account and documented proof of completing training on the software or security tool(s) or devices that individual supports in performance of cybersecurity tasks.

a. Civilian
b. Military
c. Contractor

5. On-the-Job Evaluation. This applies only to the IAT category and CSSP Specialty (except for CSSP Manager). By category or specialty (IAT and CSSP) and level (Level I, II, and III), report the number who have passed an initial on-the-job evaluation.
a. Civilian
b. Military
c. Contractor

6. Signed Privileged User Statement: This applies to the IAT category, select IAM with privilege access, and CSSP Specialty (except for CSSP Manager). By category or specialty (IAT, IAM, and CSSP) and level (Level I, II, and III), report the number with signed agreements by the individual and supervisor or management, outlining access responsibilities.
a. Civilian
b. Military
c. Contractor

7. National Security Investigation: By category or specialty (IAT, IAM, IASAE, and CSSP) and level (Level I, II, and III), report the number of cybersecurity personnel who have security investigation appropriate for assigned position.
a. Civilian
b. Military
c. Contractor

8. Qualified: By category or specialty (IAT, IAM, IASAE, and CSSP) and level (Level I, II, and III), report the number who have completed all of the requirements for their respective category and level in accordance with **Chapter 4** and of DoD 8570.01-M, Table AP3.T1.
a. Civilian
b. Military
c. Contractor

9. Waivers: Report the number of cybersecurity personnel who have approved waivers.
a. Civilian
b. Military

10. Certified not in position: Report the number of cybersecurity personnel with an approved cybersecurity certification, but not in an assigned position.
a. Civilian
b. Military
Signature Block

Attachment 5

FORMAL STATEMENT OF RESPONSIBILITES (APPLICABLE FOR CIVILIANS AND MILITARY)

A5.1. Formal Statement. The Formal Statement of Assigned Cybersecurity responsibilities may be completed using Figure A5.1. (See example identified in paragraphs 2.14.2.2., and 2.19.4. Keep document locally.

Figure A5.1. Sample Formal Statement of Assigned Cybersecurity Responsibilities.

(Appropriate letterhead)

Date

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cybersecurity Responsibilities

1. I understand I have been assigned to a cybersecurity-coded position on the [INSERT UNIT NAME HERE] Unit Manning Document (UMD). In accordance with AFMAN 17-1303, AF *Cybersecurity Workforce Improvement Program*, **Paragraphs 2.14.2.2, 2.18.3** and **2.19.4**, supervisors and members will sign a formal statement of assigned cybersecurity responsibilities. **(T-0).** Details of the UMD position number, Special Experience Identifier (SEI), Cybersecurity Workforce Category or Specialty, and Cybersecurity Workforce Level have been identified and are listed below:

UMD Position Number:
SEI Required:
Cybersecurity Workforce Category or Specialty:
Cybersecurity Workforce Level:

2. Upon being assigned, I am or may be expected to perform all or some of the cybersecurity tasks as defined in AFMAN 17-1303 **Attachment 2** for my category or specialty and level. My supervisor has reviewed with me the applicable tasks from **Attachment 2.**

3. I understand I will obtain and maintain the appropriate DoD approved cybersecurity baseline certification(s) applicable for the cybersecurity tasks assigned above and required for the above position in accordance with AFMAN 17-1303 and DoD 8570.01-M.

Member’s Signature Block Supervisor’s Signature Block

A5.2. The Consolidated Formal Statement of Assigned Cybersecurity Responsibilities and Privileged User Agreement may be completed by using Figure A5.2 as an example as identified in paragraphs 2.14.2.2, 2.18.3. and 2.19.4. The sample consolidates the statement of responsibilities and the Privileged User Agreement found in DoD 8570.01-M, Appendix 4. This document is kept locally.

Figure A5.2. Sample Consolidated Formal Statement of Assigned Cybersecurity Responsibilities.

(Appropriate letterhead)

Date

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cybersecurity Responsibilities & Privileged User Agreement

1. I understand I have been assigned to a cybersecurity-coded position on the [INSERT UNIT NAME HERE] Unit Manning Document (UMD). In accordance with AFMAN 17-1303, AF *Cybersecurity Workforce Improvement Program*, **Paragraphs 2.14.2.2**, **2.18.3** and **2.19.4**, supervisors and members will sign a formal statement of assigned cybersecurity responsibilities. Details of the UMD position number, Special Experience Identifier (SEI), Cybersecurity Workforce Category or Specialty, and Cybersecurity Workforce Level and in accordance with **Paragraph 3.3** have been identified and are listed below:

UMD Position Number:
SEI Required:
Cybersecurity Workforce Category or Specialty:
Cybersecurity Workforce Level:

2. Upon being assigned, I am or may be expected to perform all or some of the cybersecurity tasks as defined in AFMAN 17-1303 **Attachment 2** for my category or specialty and level. My supervisor has reviewed with me the applicable tasks from **Attachment 2.**

3. I understand I will obtain and maintain the appropriate DoD approved cybersecurity baseline certification(s) applicable for the cybersecurity tasks assigned above and required for the above position in accordance with AFMAN 17-1303 and DoD 8570.01-M.

4. Privileged User Agreement:

a. I understand, acknowledge and consent to the following:

1) I am accessing a U.S. Government Information System (which includes any device attached to this Information System) that is provided for U.S. Government authorized used only.

2) The U.S. Government routinely intercepts and monitors communications on this Information System for purposes including, but not limited to, penetration testing, Information Systems Security Monitoring, network operations and defense, personnel misconduct, law enforcement and counterintelligence investigations.

3) At any time, the U.S. Government may inspect and seize data stored on this Information System.

4) Communications using, or data stored on, this Information System are not private, are subject to routine monitoring, interception and search, and may be disclosed or used for any U.S. Government-authorized purpose.

5) This Information System includes security measures (e.g., authentication and access controls) to protect U.S. Government interests – not for my personal benefit or privacy.

b. I understand that access to a U.S. Government system or network is a revocable privilege, and that failure to comply with requirements is a violation of the trust extended to me and may result in one or more administrative or judicial actions such as, but not limited to: chain of command revoking access or user privileges; counseling; adverse actions under the UCMJ or criminal prosecution; discharge or loss of employment; security incident reporting; or revocation of security clearances and access.

c. I am responsible for all actions taken under my administrative or root account(s) and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will only use the privileged access granted to me to perform authorized tasks for mission related functions. I will use my general user account at all other times.

d. I will protect the administrative or root account(s), passwords, and other authenticator(s) to the highest level of data or resource it secures.

e. I will not share the administrative or root account(s), passwords, and other authenticator(s) entrusted for my use.

f. I will not create or elevate privileged rights of others, share permissions to Information Systems not authorized, nor allow others access to Information Systems or networks under my privileged account.

g. If I work in a capacity where I have rights to remotely log into users' systems, I will ensure they are positively informed of my presence prior to taking any actions on their systems.

h. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate security representatives.

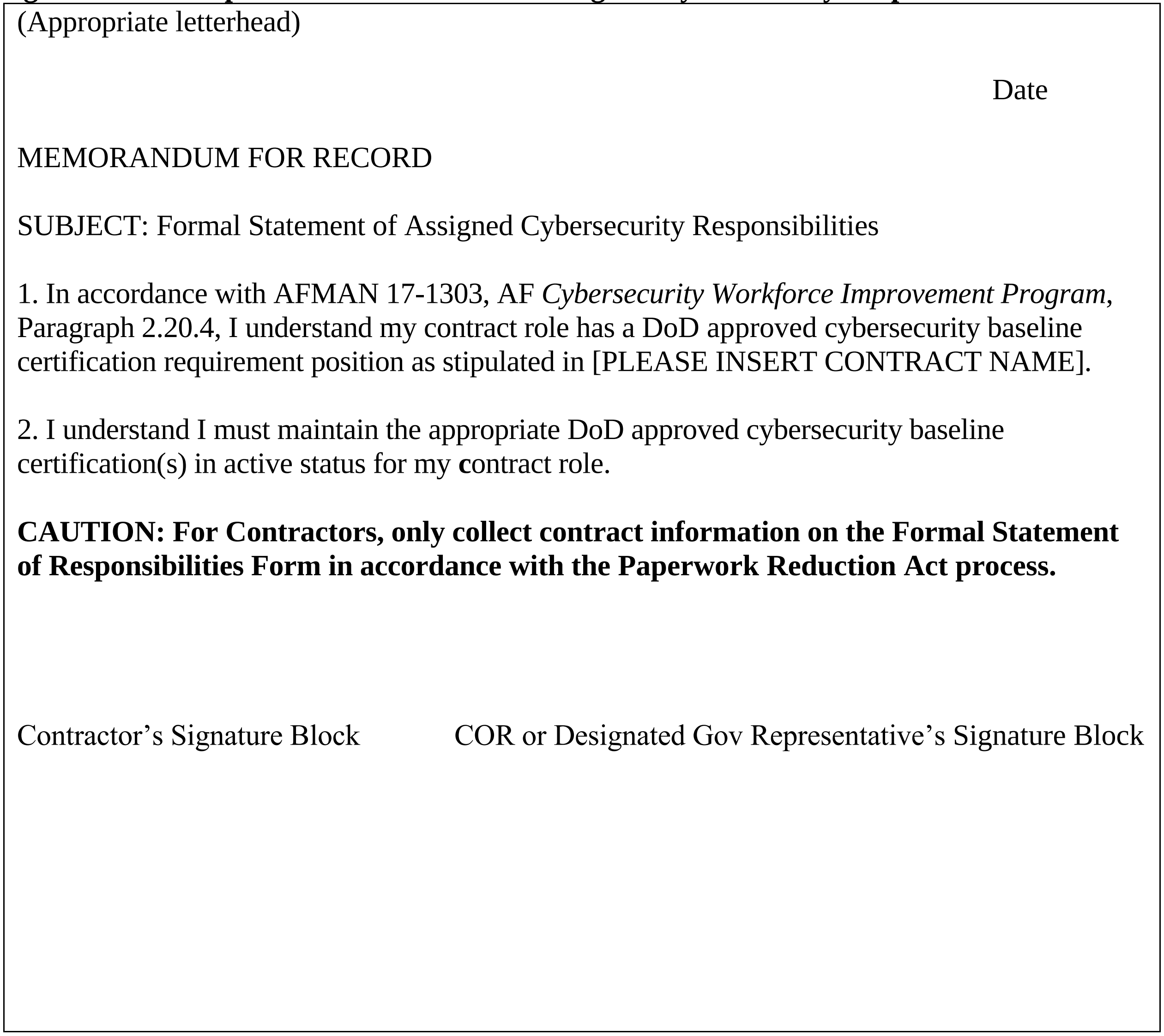
Member's Signature Block Supervisor's Signature Block

Attachment 6

FORMAL STATEMENT OF RESPONSIBILITIES (APPLICABLE FOR CONTRACTORS)

A6.1. The Formal Statement of Assigned Cybersecurity responsibilities for contractors may be completed by using Figure A6.1 as an example as identified in paragraphs 2.14.11.2, and 2.20.4. The document is kept locally.

Figure A6.1. Sample Formal Statement of Assigned Cybersecurity Responsibilities



(Appropriate letterhead)

Date

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cybersecurity Responsibilities

1. In accordance with AFMAN 17-1303, AF *Cybersecurity Workforce Improvement Program*, Paragraph 2.20.4, I understand my contract role has a DoD approved cybersecurity baseline certification requirement position as stipulated in [PLEASE INSERT CONTRACT NAME].

2. I understand I must maintain the appropriate DoD approved cybersecurity baseline certification(s) in active status for my contract role.

CAUTION: For Contractors, only collect contract information on the Formal Statement of Responsibilities Form in accordance with the Paperwork Reduction Act process.

Contractor's Signature Block COR or Designated Gov Representative's Signature Block