DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFMAN17-1303_AFGM2018-01
23 July 2018

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Air Force Guidance Memorandum to AFMAN33-285 *CYBERSECURITY WORKFORCE IMPROVEMENT PROGRAM*

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes AFMAN 33-285 *Cybersecurity Workforce Improvement Program*, 20 Mar 2015 Information. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. The authorities to waive wing/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 requestors commander for non-tiered compliance items.

As a result of the publication of Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, AFMAN 33-285 is hereby renumbered as AFMAN 17-1303, *Cybersecurity Workforce Improvement Progra*m.

Ensure that all records created as a result of processes prescribed in this publication are maintained as evidentiary documents supporting annual financial audits, or otherwise maintained and disposed of in in accordance with Air Force Manual 33-363, Management of Records, and the Air Force Records Disposition Schedule located in the Air Force Records Information Management System.

This Memorandum revises AFMAN 17-1303 by the following modifications:

1. Removing roles and responsibilities for Unit Training Managers (UTMs).

2. Aligning cybersecurity baseline certification requirements for Wing Communications Security positions with applicable National Security Agency (NSA) directives and policies.

3. Mandating certification requirement for those civilian/military/contractors performing in senior software developer, senior software subject expert or senior software tester role(s).

4. Modifying special experience identifier (SEI) lists for civilians and military (officer and enlisted).

5. Clarifying the computing environment/operating system training completion certificate requirement, including acceptable documentation.

6. Revising the certification determination guide (Attachment 2), to include redefining cybersecurity tasks for Technical Category and Management Category as well as defining for Computer Network Defense – Service Provider Specialty and Information Assurance System Architect and Engineer Specialty.

7. Updating references, terms, and links.

This guidance applies to all AF civilian, military, and contractor (US citizens, Foreign Nationals [FNs], and Local Nationals [LNs]) personnel performing cybersecurity functions:

1.1. Changed to read: Objectives. This manual implements DoD Directive (Dodd) 8140.01, *Cyberspace Workforce Management* and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, identifying AF requirements, roles, and responsibilities. The primary objective of the Air Force (AF) Cybersecurity Workforce Improvement Program (WIP) is to train, educate, certify, and qualify personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and dispose/retire DoD Systems.

All authorized users of DoD Information Systems /Platform Information Technology systems such as those requiring access to the Air Force Network (AFNet), consisting of the Non-Classified Internet Protocol Router (NIPR) and Secret Internet Protocol Router (SIPR) networks, must receive initial cybersecurity user awareness training as a condition of access to an IS in accordance with DoD 8570.01-M, Paragraph C6.2.2.; thereafter, all users will complete annual cybersecurity user awareness refresher training **(T-0)**. In accordance with AFI 36-2201, *Air Force Training Program*, Paragraph 7.3.1.3, the Advanced Distributed Learning Service (ADLS) is the preferred method for this training. ADLS can be found at this link: **https://golearn.csd.disa.mil/kc/rso/login/ADLS_login.asp**. As a secondary method, this training can be found on the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) portal: **http://iase.disa.mil/eta/Pages/index.aspx**. Details on network/system account access and management processes can be found in AFMAN 17-1301, *Computer Security (COMPUSEC)*.

This manual also identifies AF cybersecurity workforce positions, certification and qualifications requirements, and provides policy on cybersecurity workforce reporting, metrics and validation. Unless noted, the cybersecurity position requirements (e.g., certification, training, etc.) specified in this manual are the minimum required. Commanders are authorized to increase requirements to reflect specific duties and or function(s).

1.3. Changed to read: Applicability. Cybersecurity workforce functions and associated DoD approved baseline cybersecurity certifications are identified in DoD 8570.01-M by category (IAT and IAM) or specialty (CND-SP and IASAE). The cybersecurity workforce positions on a unit manning document (UMD) will reflect the certification required using established special experience identifiers (SEIs). The cybersecurity workforce consists of all civilian, military, and contractors performing a cybersecurity function IAW DoD 8570.01-M, requires possession of a current/valid cybersecurity baseline certification, and all Airmen who are required to possess a valid/current baseline cybersecurity certifications as a precondition of their respective Air Force Specialty Code (AFSC). This manual applies to all AF civilian, military, and contractor (US citizens, Foreign Nationals [FNs], and Local Nationals [LNs]) personnel performing cybersecurity functions or tasks IAW DoD Chief Information Officer (DoD CIO) policies. AFMAN 17-1303 compliance is required for the Intelligence Community (IC) and Special Access Program (SAP) unless AFMAN conflicts with the Office of Director of National Intelligence (ODNI) or the DoD Director, Special Access Programs Central Office (DoD SAPCO) directives respectfully. When in conflict, the ODNI and DoD SAPCO Guidance take precedence for the IC and SAP community. Although DoD 8570.01-M requirements have been vetted through OSD legal channels and with National Unions, DoD CIO has strongly recommended continuous engagements with appropriate local parties such as the local or country Human Resources section of the Office of Personnel Management (OPM) or local unions.

2.4.3. Deleted.

2.4.4. Deleted.

2.4.5. Deleted.

2.4.6. Deleted.

2.4.7. Deleted.

2.4.8. Deleted

2.12. Deleted.

2.13.3. Changed to read: Will report statistics on Wing's cybersecurity workforce personnel compliance. SAF/CIO A6 will provide the reporting instructions (**T-1)**.

2.17. Deleted.

2.19.6. Changed to read: Will authorize release of cybersecurity baseline certification data to DOD via DMDC IAW DoD 8570.01-M, Paragraphs C2.3.12 **(T-0)**. The authorization release can be found on milConnect portal under the DoD Workforce Certification workspace: **https://milconnect-pki.dmdc.osd.mil/milconnect/protected/portlet/dwc/**

3.2.2.3. Changed to read: AM Level III. An individual in an IAM Level III position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** in accordance with DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. Examples of an IAM Level III could include the AF Chief Information Security Officer (CISO), SAF/CIO A6 cybersecurity staff personnel, several MAJCOM cybersecurity staff positions, Security Control Assessor, and ISSM for Information Systems/Platform Information Technology system(s) providing enterprise capabilities and/or services to AF end users worldwide **(T-1)**.

3.2.3. Changed to read: AF Chief Information Security Officer (CISO). The AF Chief Information Security Officer is the official responsible for directing the Air Force's cybersecurity program on behalf of the AF CIO. The AF Chief Information Security Officer will attain and maintain an IAM Level III cybersecurity baseline certification. AF centralized funds will pay for certification exam and associated maintenance fees **(T-1)**.

3.2.5.1. Changed to read: Security Control Assessor (SCA). The SCA (formerly called Certifying Authority [CA]) is the senior official having the authority and responsibility for the assessment of an IS/ PIT system. The SCA roles and responsibilities are addressed in AFI 17-101, *Risk Management Framework for Air Force Information Technology (IT)*. SCAs will attain and maintain a DoD approved IAM Level III cybersecurity baseline certification (**T-1**). Also, it is highly recommended SCAs should both complete the AO 9training module and attain the Committee on National Security Systems Instruction (CNSSI) 4016 certificate, for supplemental training on the AO responsibilities and risk analysis/mitigation, respectively.

3.2.8. Changed to read: Information System Security Managers (ISSMs) for IS/PIT System. An ISSM for an IS/PIT system creates and/or oversees the cybersecurity program to include cybersecurity architecture, requirements, personnel, policies, processes and procedures. The ISSM acts as the primary cybersecurity technical advisor to the AO. As such, it is imperative that the ISSM have the appropriate foundational knowledge of cybersecurity best practices and risk management commensurate to the criticality of information stored and/or processed on the ISs/PIT systems. For ISs/PIT systems providing enterprise capabilities and/or services to AF end users worldwide, the ISSM will attain and maintain, at a minimum, an IAM Level III cybersecurity baseline certification **(T-1)**. For ISs/PIT systems that are networked and interconnected, but do not provide enterprise capabilities and/or services to AF end users worldwide, the ISSM will attain and maintain, at a minimum, an IAM Level II cybersecurity baseline certification **(T-1)**. Roles and responsibilities of ISSMs are addressed in AFI 17-101 and AFI 17-

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

3.2.11.2. Changed to read: 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/Platform Information Technology system.

3.2.11.4. Changed to read: Exempted individuals will be classified as an "Authorized User" (**T-1**). The AF CISO or CISO's designated representative will provide the instructions to request network/system account via DD Form 2875 process for these individuals for the affected Information System/Platform Information Technology system.

3.2.11.5. Changed to read: The Program Management Office/unit must complete and document in memo format an annual (i.e., occurring on anniversary date of exemption approval) validation of exemption memo to include personnel and Information System/Platform Information Technology system **(T-1)**. The ISSM will sign the memo and route to the MAJCOM and Authorizing Official for in-turn signatures **(T-2)**. Program Management Offices 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 of the affected Information System/Platform Information Technology system **(T-1)**.

3.2.12. Changed to read: Software Developer/Engineer/Programmer Supporting Information System/Platform Information Technology System. A software developer/engineer/programmer designs, creates, modifies, integrates, tests, and/or maintains computer applications, software, or specialized utility programs for use on Air Force networks/systems. It is critical cybersecurity is integrated into the development, sustainment and disposal of AF data, networks and systems. DoD is working to transform the competencies of its software developers/engineers/programmers, striving for a more qualified workforce, using the DoD Cyber Workforce Framework:

3.2.12.1. Changed to read: Civilian and Military

3.2.12.1.1. Changed to read: Senior Software Development Roles: The Program Management Offices/units must identify and record positions as IASAE Level II for those civilians and military who are performing in senior software developer role, senior software consultant/subject matter expert (SME) role, and/or senior software tester role(s) in accordance with

Attachment 2. Affected individuals will possess a cybersecurity baseline certification on the DoD approved listing. Individuals in these senior roles should have at least four years of software development experience. Additionally, 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). The knowledge areas must include, but not limited to, secure software requirements and design, secure coding techniques, and secure software deployment strategies. The Program Management Offices/units must comply by 1 Jul 2019 for all affected positions to be coded as well as personnel certified (**T-1**). Table A2.5 includes list of representative tasks for the senior software development roles.

3.2.12.1.2. Changed to read: Remaining Software Development Roles: For every other civilian and military member performing in a software developer/engineer/programmer role, but not in a senior software development role described to Paragraph 3.2.12.1.1, the following conditions will apply annually (effective 1 Jul 2019):

3.2.12.1.2.1. Added: Civilian/Military will complete 40 training hours. This training must include elements of cybersecurity as well as programming/software language. The Program Management Office/unit has the flexibility to define training content/topics. Examples of acceptable training: formal, computer based training, web-based, and classroom instruction **(T-3)**.

NOTE: Cybersecurity training must be in addition to annual cybersecurity user awareness training. Suggested cybersecurity training topics: cybersecurity principles, cyber threats and vulnerabilities, or secure coding practices.

3.2.12.1.2.2. Added: The Program Management Office/unit must document/track successful completion of training.

3.2.12.1.2.2.1. Added: Documentation must include name of individual trained, title of training completed, and date training was completed. Examples of acceptable documentation: digital/printed certificates; sanitized (i.e., all personally identifiable information except for name of individual and dates of training completion are redacted) copy of transcript; and memo for record annotating training completion signed by individual’s supervisor **(T-1)**.

3.2.12.1.2.2.2. Added: Documentation can be stored digitally/electronically or in paper format.

3.2.12.2. Changed to read: Contractors

3.2.12.2.1. Added: Senior Software Development Roles: Effective 1 July 2019, The requirements documents, Performance Work Statements or Statements of Work, for all new contracts, modified contracts, and contracts beginning with a new option years must include the stipulation that all contractors performing in senior software developer role, senior software consultant/subject matter expert (SME) role, and/or senior software tester role(s) in accordance with Attachment 2 will be classified as IA System Architect and Engineer Level II. Table A2.5 includes list of representative tasks for the senior software development roles. Affected contractors will possess a cybersecurity baseline certification on the DoD approved listing. Individuals in these senior roles should have at least four years of software development experience. Additionally, 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). The knowledge areas must include, but not limited to, secure software requirements and design, secure coding techniques, and secure software deployment strategies **(T-1).**

3.2.12.2.2. Added: Remaining Software Development Roles: Effective 1 Jul 2019, the requirements documents, Performance Work Statement, or Statements of Work for all new contracts, modified contracts, and contracts beginning with a new option year must include the following stipulations for all contractors performing in a software developer/engineer/programmer role, but not in a senior software development role as described in **Paragraph 3.2.12.1.1**:

3.2.12.2.2.1. Added: Contractors will complete 40 training hours. This training must include elements of cybersecurity and a programming/software language. Cybersecurity training must be in addition to annual cybersecurity user awareness training. The PMO/unit has the flexibility to decide training content/topics. Suggested cybersecurity topics: cybersecurity principles, cyber threats and vulnerabilities or secure coding. Examples of acceptable training: formal, computer based training, web-based, and classroom instruction **(T-3)**.

3.2.13.2. Changed to read: Wing Communications Security Accounts with Key Management Infrastructure Capabilities: Only individuals (civilian, military, or contractor) in either the client platform administrator or client platform security officer position will attain and maintain at a minimum, an IAT Level I cybersecurity baseline certification in accordance with NSA IAD DOC-042-12 **(T-0)**. No other Communications Security position has a mandatory certification requirement. NOTE: Assigned military personnel (e.g., those in 3D0X3 Air Force Specialty Code) must still meet, also, their respective AFSC mandatory certification requirements **(T-1).**

3.2.14. Deleted

Table 3.1. Changed to read: Civilian SEIs (Positions Coded with Equivalent Enlisted Air Force Specialty Codes.

Certification Category/Specialty and Level	**Civilian SEIs for Positions Coded with an Enlisted Air Force 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
IA System Architect and Engineer Level I	402
IA System Architect and Engineer Level II	403
IA System Architect and Engineer Level III	404
Computer Network Defense – Service Provider Analyst	872
Computer Network Defense – Service Provider Infrastructure Support	873
Computer Network Defense – Service Provider Incident Responder	874
Computer Network Defense – Service Provider Auditor	875
Computer Network Defense – Service Provider Manager	876

Table 3.2. Changed to read: Civilian SEIs (Positions Coded with Equivalent Officer AFSCs).

Certification Category/Specialty and Level	**Computer Systems SEIs** *See Table 3.2. NOTE	**Operations SEIs** *See Table 3.2. 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
IA System Architect and Engineer Level I	CO1	OO1
IA System Architect and Engineer Level II	CO2	OO2
IA System Architect and Engineer Level III	CO3	OO3
Computer Network Defense - Service Provider Analyst	CO4	OO4
Computer Network Defense - Service Provider Auditor	CO5	OO5
Computer Network Defense - Service Provider Incident Responder	CO6	OO6
Computer Network Defense - Service Provider Infrastructure Support	CO7	OO7
Computer Network Defense - Service Provider Manager	CO8	OO8

Table 3.2. Added: NOTE

*** Table 3.2. 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.

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

3.4.2.2. Changed to read: The Air Force Enlisted Classification Directory has the current list of enlisted SEIs and is located on the myPers portal: **https://gum-crm.csd.disa.mil/app/login/redirect/home**

3.4.2.3. Changed to read: The AF Officer Classification Directory includes current list of activity codes and SEIs as well as is located on the myPers portal: **https://gum-crm.csd.disa.mil/app/login/redirect/home**

Table 3.3. Changed to read: Enlisted SEIs.

Certification Category/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
IA System Architect and Engineer Level I	402
IA System Architect and Engineer Level II	403
IA System Architect and Engineer Level III	404
Computer Network Defense - Service Provider Analyst	872
Computer Network Defense - Service Provider Infrastructure Support	873
Computer Network Defense - Service Provider Incident Responder	874
Computer Network Defense - Service Provider Auditor	875
Computer Network Defense - Service Provider Manager	876

Table 3.4. Added: Officer SEIs.

Certification Category/Specialty and Level	**Computer Systems SEIs** ***See Table 3.4. NOTE**	**Operations SEIs** ***See Table 3.4. 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
IA System Architect and Engineer Level I	CO1	OO1
IA System Architect and Engineer Level II	CO2	OO2
IA System Architect and Engineer Level III	CO3	OO3
Computer Network Defense – Service Provider Analyst	CO4	OO4
Computer Network Defense – Service Provider Auditor	CO5	OO5
Computer Network Defense – Service Provider Incident Responder	CO6	OO6
Computer Network Defense – Service Provider Infrastructure Support	CO7	OO7
Computer Network Defense – Service Provider Manager	CO8	OO8

Table 3.4. Added: NOTE

***Table 3.4. 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

3.4.3.2. Deleted.

4.2. Changed to read: Computing Environment/Operating System Training Completion Requirement. All civilians, military, and contractor personnel possessing an IAT certification, a Computer Network Defense – Service Provider (except for Computer Network Defense – Service Provider Manager position) specialty certification, or a privileged access account will complete training (e.g., formal, computer based training, web-based, classroom instruction, on-the-job training, etc.) on the operating system(s) and/or security device(s)/service(s)/tool(s) the Program Management Office/unit supports **(T-0)**. The Program Management Offices/units have the flexibility to decide what training, including content and length, is adequate to meet this requirement.

4.2.1. Changed to read: Documentation. The Program Management Office/unit must document individual's successful completion of training. At minimum, the documentation must include name of individual trained, title of training completed, and date training was completed. Documentation can be stored digitally/electronically or in paper format, but must readily accessible, especially during audits or inspections. Examples of acceptable documentation could include digital/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)**.

5.2.1. Changed to read: The AF has developed a preferred list, based on the DoD approved cybersecurity baseline certifications. The AF Preferred List can be found at this link: **https://cs2.eis.af.mil/sites/13057/A6S/A6SF/8570/default.aspx**. In consultation with AF subject matter experts, SAF/CIO A6 staff will review the preferred list and make changes, as necessary **(T-1)**.Those certifications on the AF preferred list have priority for funding.

5.3. Changed to read: Minimum Cybersecurity Baseline Certification Requirement for Select Enlisted AFSCs. Multiple military AFSCs have mandatory certification requirements as defined in the Air Force Enlisted Classification Directory. Refer to the latest version of the Air Force Enlisted Classification Directory for requirement details. **Note:** A higher level certification than mandated by AFSC may be required for assigned position.

5.3.1. Changed to read: Exam. AF centralized funds will pay for one (1) exam voucher at the specified AFSC requirement unless member occupies an assigned position with different/higher cybersecurity requirements. AF centralized funds 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/specialty, or multiple cybersecurity baseline certifications.

5.3.1.1. Deleted.

5.3.1.2. Deleted.

5.7. Changed to read: Continuing Education Units (CEUs). DoD approved cybersecurity baseline certifications require CEUs to stay current. Commercial certification providers define the criteria for acceptable continuing education units. All certification holders (civilians, military, and contractors) will adhere to CEU policies set by their respective certification provider(s) IAW DoD 8570.01-M, Paragraph C3.2.3.7 **(T-0)**. Some commercial certification providers may allow CEUs for work experience that is documented and verified. Also, CBTs may count toward CEUs (please check with the commercial certification provider) and are available via various DoD resources such as the AF e-Learning program for civilians and military.

5.8.3. Changed to read: Civilian, military, and contractor personnel will authorize a new certification release, whenever a certification is issued or renewed, to DoD/DMDC IAW DoD 8570.01-M, Paragraph C2.3.12 **(T-0)**. Personnel can access and submit release via DWCA on the DMDC portal: **https://milconnect-pki.dmdc.osd.mil/milconnect/protected/portlet/dwc/**.

5.9.2. Changed to read: 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 attained, as indicated in the Enlisted or Officer Classification Directory **(T-1)**. 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, it is submitted to the appropriate servicing personnel function (e.g., Force Support Squadron, Military Personnel FPF, or equivalent) for assignment to member's personnel record.

6.1. Changed to read: Initial Skills Training. Cyberspace Defense Operations enlisted personnel (1B4), various Cyberspace Support enlisted personnel (3D), and Cyberspace Operations officers (17X) are provided initial cybersecurity certification training at the schoolhouses. Civilians and military personnel not in an Air Force Specialty Code listed can obtain training via distributive/online learning or unit-funded training course

6.1.1 Deleted.

6.1.1.1. Deleted.

6.1.1.2. Deleted.

6.1.1.3. Deleted.

6.1.1.4. Deleted.

6.1.1.5. Deleted.

6.1.1.6. Deleted.

6.1.2. Deleted.

6.1.3. Deleted.

6.3. Changed to read: Authorizing Official Training. The Authorizing Official will attain training through the CAC-enabled DoD Authorizing Official Course located on the IASE portal: **http://iase.disa.mil/eta/Pages/index.aspx (T-0)**.

Attachment 1 Changed to read:

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5, U.S.C., Section 552a, as amended, *The Privacy Act of 1974*

National Defense Authorization Act for Fiscal Year 2013

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

Committee on National Security Systems Instructions 4016, *National Information Assurance Training Standard for Risk Analysts*, 1 November 2005

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

DoD Instruction (DoDI) 1336.05 Change 2, *Automated Extract of Active Duty Military Personnel Records*, 31 March 2015

DoDI 5000.02 Change 3, *Operation of the Defense Acquisition System*, 10 August 2017

DoDI 7730.64, *Automated Extracts of Manpower and Unit Organizational Element Files*, 11 December 2004

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DODI 8510.01 Change 2, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 28 July 2017

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

DoD Manual 5200.02, *Procedures for the DoD Personnel Security Program (PSP)*, 3 April 2017

Air Force Instruction (AFI) 17-100, *Air Force Information Technology Service Management*, 16

September 2014

AFI 17-130, *Cybersecurity Program Management*, 31 August 2015

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 2 February 2017

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

AFI 36-701, *Labor Management Relations*, 6 April 2017

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

AFI 36-2201, *Air Force Training Program*, 15 September 2010

AFI 38-101, *Air Force Organization*, 31 January 2017

Air Force Manual (AFMAN) 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

AFMAN 33-363, *Management of Records*, 1 March 2008

Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 17-2, *Cyberspace Operations*

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

Replace International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17024, *Conformity Assessment – General Requirements for Bodies Operating Certification of Persons*, 3 July 2012

Adopted Forms

DD Form 2875, System Authorization Access Request (SAAR), August 2009

AF Form 847, Recommendation for Change of Publication, 22 September 2009

AF Form 2096, Classification/On-the-Job Training Action, 26 March 2014

Abbreviations and Acronyms

AF — Air Force

AFSC — Air Force Specialty Code

AFPERS — Air Force Personnel Services

ANG — Air National Guard

AFRC — Air Force Reserve Command

AO — Authorizing Official

BI — Background Investigation

CE — Computing Environment

CEU — Continuing Education Unit

CFM — Career Field Manager

CIA — Confidentiality, Integrity, and Availability

CIO — Chief Information Officer

CND — Computer Network Defense

CND-A — Computer Network Defense Analyst

CND-AU —Computer Network Defense Auditor

CND-IR — Computer Network Defense Incident Responder

CND-IS — Computer Network Defense Infrastructure Support

CND-SP — Computer Network Defense Service Provider

CND-SPM — Computer Network Defense Service Provider Manager

CNSSI — Committee on National Security Systems Instruction

CO — Contracting Officer

CPCN — Civilian Position Control Number

CPD — Core Personnel Document

COCOM — Combatant Command

CSSLP — Certified Secure Software Lifecycle Professional

DCPDS — Defense Civilian Personnel Data System

DEERS — Defense Eligibility Enrollment Reporting System

DISA — Defense Information Systems Agency

DMDC — Defense Manpower Data Center

DoD — Department of Defense

DoD CIO — DoD Chief Information Officer

DoDIN — DOD Information Network

DoD SAPCO — DoD Director, Special Access Programs Central Office

DRU — Direct Reporting Units

DFARS — Defense Federal Acquisition Regulation Supplement

FISMA — Federal Information Security Management Act

FN — Foreign National

FOA — Field Operating Agency

HBSS — Host Base Security System

IA — Information Assurance

IAM — Information Assurance Management Category

IASE — Information Assurance Support Environment

IAT — Information Assurance Technical Category

IC — Intelligence Community

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

INWT — Intermediate Network Warfare Training

IS — Information System

(ISC)2 — International Information Systems Security Certification Consortium

ISO/IEC — International Organization for Standardization/International Electro-technical Commission

ISSO — Information System Security Officer

ISSM — Information System Security Manager

IT — Information Technology

LN — Local National

MAJCOM — Major Command

MILPDS — Military Personnel Data System

MPCN — Manpower Position Control Number

MPES — Manpower Programming and Execution System

NE — Network Environment

ODNI — Office of Director of National Intelligence

OE — Operating Environment

OJE — On-the-Job Evaluation

OPM — Office of Personnel Management

OSD — Office of the Secretary of Defense

PD — Position Description

POM — Program Objective Memorandum

SAP — Special Access Program

SEI — Special Experience Identifier

SP — Service Provider

SRG — Security Recommendation Guide

SSBI — Single Scope Background Investigation

UCT — Undergraduate Cyberspace Training

UMD — Unit Manning Document

UTM — Unit Training Manager

WCO — Wing Cybersecurity Office

WIP — Workforce Improvement Program

Attachment 2 Changed to read:

AF Cybersecurity Workforce Position Certification Determination Guide

Actions captured below are commensurate with the role, position, duty description, responsibilities and privileges of assigned personnel.

A2.1. Added: Technical Category Positions.

Table A2.1. Changed to read: Technical Category.

Duties	**IAT Level I**	**IAT Level II**	**IAT Level III**
Conduct general system tasks on client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.). NOTE: Example of general system tasks on end user device(s): • Create/modify user account • Create/modify login scripts • Download/install standard functional drivers and operating system • Install peripherals (printers, scanners, etc.) • Install/update security drivers/software, including definitions • Lock/unlock user account • Modify account privilege(s) • Perform backups • Reset user password • Run queries • View account properties • View queries	X		

Conduct general system management on host(s) or server(s), including an Information System or Platform Information Technology system located on the Air Force Information Network (AFIN). The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100. The Air Force core missions: 1. Air and Space Superiority 2. Intelligence, Surveillance, and Reconnaissance 3. Rapid Global Mobility 4. Global Strike 5. Command and Control (C2) NOTE: General system management can involve performing one or more of the following tasks: • Create /modify e-mail group mailbox • Create administrator accounts • Create/delete e-mail account • Create/modify login scripts • Create/modify user account • Download/install standard functional drivers and operating system • Install peripherals (e.g., printers, scanners) • Install/update security drivers/software, including definitions • Lock/unlock user account • Modify account privilege(s) • Modify login scripts • Perform backups • Reset user password • Reset administrator account password • Run queries • View account properties **EXCEPTION: Select personnel providing unique direct support to medical community. SAF/CIO A6 and AF/SG staff will identify affected personnel who will be classified as "IAT Level I."**	**X***** *****IAT Level I Exception: Applicable only to Select Personnel in accordance with SAF/CIO A6 and AF/SG coordinations.**	X	

Duties	IAT Level I	IAT Level II	IAT Level III
Has access rights to network security devices and/or tools such as, but not limited to, routers, switches firewalls, intrusion detection/prevention systems, host based security system, etc. The network security devices/tools do not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.		X	
Conduct technical audits/validations of security controls for Information System/Platform Information Technology system located on the AFIN. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X

Duties	IAT Level I	IAT Level II	IAT Level III
Conduct general system management on host(s) or server(s), including an Information System or a Platform Information Technology system located on the AFIN. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100. NOTE: General system management involves performing one or more of the following tasks: • Create /modify e-mail group mailbox • Create administrator accounts • Create/delete e-mail account • Create/modify login scripts • Create/modify user account • Download/install standard functional drivers and operating system • Install peripherals (printers, scanners, etc.) • Install/update security drivers/software, including definitions • Lock/unlock user account • Modify account privilege(s) • Modify login scripts • Perform backups • Push security software/ updates • Reset user password • Reset administrator account password only • Run queries • Update antivirus definitions • View account properties			X

Duties	**IAT Level I**	**IAT Level II**	**IAT Level III**
Has access rights to network security devices and/or tools such as routers, firewalls, intrusion detection/prevention systems, and Host Based Security System, etc. These security devices/tools are supporting a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.			X

A2.1. Added: Management Category.

Table A2.2. Changed to read: Management Category.

Duties	IAM Level I	IAM Level II	IAM Level III
Assist in the development of cybersecurity assessment and authorization documentation.	X		
Collect and maintain data needed to meet server cybersecurity reporting requirements.	X		
Develop/modify cybersecurity program plans and requirements for client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		
Develop procedures to ensure system users are aware of their cybersecurity responsibilities before granting access to Information Systems/Platform Information Technology system(s).	X		
Ensure system security configuration guidelines are followed.	X		
Ensure cybersecurity requirements are appropriately identified for client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) only	X		
Monitor system performance and review for compliance with security and privacy requirements on client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		
Recognize a possible security violation and take appropriate action to report the incident, as required.	X		
Supervise or manage implementation of protective or corrective controls/measures when a cybersecurity incident or vulnerability is discovered or reported.	X		
Use federal and organization specific published documents to manage operations on client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		

Duties	IAM Level I	IAM Level II	IAM Level III
Advise the Authorizing Official of any changes to the cybersecurity posture of an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Assist in the gathering and preservation of evidence used in the prosecution of computer crimes.		X	
Conduct security assessment and correct security weaknesses on an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Develop cybersecurity requirements for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IAM Level I	IAM Level II	IAM Level III
Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.		X	
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 a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Ensure that compliance monitoring occurs, and review results of such monitoring of an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IAM Level I	IAM Level II	IAM Level III
Ensure that cybersecurity inspections, tests, and reviews are coordinated for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Ensure that software, hardware, and firmware comply with appropriate security configuration guidelines, policies, and procedures for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Ensure recovery processes are monitored and that cybersecurity features and procedures are properly restored for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IAM Level I	IAM Level II	IAM Level III
Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
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	
Identify alternative cybersecurity strategies for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system, does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Monitor contract performance and periodically review deliverables for conformance with contract requirements related to cybersecurity and privacy for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IAM Level I	IAM Level II	IAM Level III
Oversee the preparation of cybersecurity assessment and authorization documentation for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the cybersecurity of an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Provide leadership and direction to personnel supporting an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Recommend resource allocations required to securely operate and maintain an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.		X	

Duties	IAM Level I	IAM Level II	IAM Level III
Review security controls and safeguards to determine if security concerns identified in the approved plan have been fully addressed in an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.		X	
Support assessment of security controls and conduct initial remediation actions in preparation for system authorization using DoD assessment procedures such as Security Recommendation Guides & Security Technical Implementation Guides.		X	
Advise the AO of changes to the cybersecurity posture of an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Approve cybersecurity assessment and authorization documentation.			X
Analyze, develop, approve, and issue cybersecurity policies for AF networks or Information System/Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X

Duties	IAM Level I	IAM Level II	IAM Level III
Analyze identified cybersecurity strategies and select the best approach or practice for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.			X
Develop the Continuity of Operations Plan for Information Systems/Platform Information Technology system(s). The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Ensure information ownership responsibilities are established for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.			X
Ensure that protection and detection capabilities are acquired or developed for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X

Duties	IAM Level I	IAM Level II	IAM Level III
Ensure that security related provisions of the system acquisition documents meet all identified cybersecurity needs for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Evaluate and approve development efforts to ensure that baseline cybersecurity safeguards are appropriately installed for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Evaluate cost benefit, economic and risk analyses for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.			X
Evaluate proposals to determine if proposed cybersecurity solutions effectively address requirements for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X

Duties	IAM Level I	IAM Level II	IAM Level III
Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Identify IT cybersecurity program implications of new technologies or technology upgrades.			X
Interpret and/or approve cybersecurity requirements relative to the capabilities of new information technologies.			X
Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of cybersecurity program for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Monitor and evaluate the effectiveness of security posture for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.			X

Duties	IAM Level I	IAM Level II	IAM Level III
Oversee the preparation of cybersecurity assessment and authorization documentation for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Review security controls and safeguards to determine if security concerns identified in the approved plan have been fully addressed in an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Supervise technical audits/validations of security controls for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Take action as needed to ensure that accepted products/tools meet Common Criteria requirements.			X

A2.3. Added: IA Workforce System Architecture and Engineering (IASAE) Specialty

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

Duties	IA System Architect and Engineer Level I	IA System Architect and Engineer Level II	IA System Architect and Engineer Level III
Assess threats and vulnerabilities on client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		
Define client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) cybersecurity requirements.	X		
Design, develop, and/or implement cybersecurity architecture for client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		
Design, develop, and/or implement cybersecurity/cybersecurity-enabled products, services, and/or solutions for client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.).	X		
Design, develop, recommend, and/or implement countermeasures/mitigations to client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) vulnerabilities.	X		
Test and evaluate products, services, solutions security and vulnerability countermeasures/mitigations to client/end user device(s) (e.g., desktop, handheld, laptop, smartphone, workstation, etc.) only configuration.	X		
Assess threats and vulnerabilities to an Information System or a Platform Information Technology system that does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IA System Architect and Engineer Level I	IA System Architect and Engineer Level II	IA System Architect and Engineer Level III
Define security requirements for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.		X	
Design, develop, and/or implement security architecture for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.		X	
Design, develop, and/or implement cybersecurity/cybersecurity-enabled products, services, and/or solutions for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.		X	
Ensure implementation of cybersecurity policies for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system does not provide either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.		X	

Duties	IA System Architect and Engineer Level I	IA System Architect and Engineer Level II	IA System Architect and Engineer Level III
Test and evaluate products, services, solutions security and vulnerability countermeasures/mitigations.		X	
Assess threats and vulnerabilities to an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner or an enterprise core service as defined in AFI 17-100.			X
Define security requirements for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Design, integrate, test and/or evaluate cross domain solutions.			X
Design, develop, and/or implement security architecture for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Design, develop, and/or implement security architectures supporting multilevel security requirements such as the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).			X

Duties	**IA System Architect and Engineer Level I**	**IA System Architect and Engineer Level II**	**IA System Architect and Engineer Level III**
Design, develop, and/or implement cybersecurity/cybersecurity-enabled products, services, and/or solutions for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either supporting a "mission critical capability" as determined by the Authorizing Official or an enterprise core service as defined in AFI 17-100.			X
Design, develop, and/or implement security countermeasures/mitigations to vulnerabilities of an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X
Develop interface specifications for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information Systems Owner; or an enterprise core service as defined in AFI 17-100.			X
Ensure implementation of cybersecurity policies for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner; or an enterprise core service as defined in AFI 17-100.			X

Duties	**IA System Architect and Engineer Level I**	**IA System Architect and Engineer Level II**	**IA System Architect and Engineer Level III**
Integrate and/or implement cross domain solutions.			X
Test and evaluate products, services, solutions security and vulnerability countermeasures/mitigations for an Information System or a Platform Information Technology system. The Information System/Platform Information Technology system provides either a capability deemed significantly crucial to the execution of an Air Force core mission as determined by the Information System Owner or an enterprise core service as defined in AFI 17-100.			X

A2.4. Added: Computer Network Defense – Service Provider Specialty Positions.

Table A2.4.1. Added: Computer Network Defense – Service Provider Analyst Position.

(Primary Focus: Personnel Assigned to Units Performing Computer Network Defense – Service Provider Missions)

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

Table A2.4.2. Added: CND-SP Auditor Position.

(Primary Focus: Personnel Assigned to Units Performing Computer Network Defense – Service Provider Missions)

Duties	Computer Network Defense – Service Provider <u>Auditor</u>
Conduct/support authorized penetration testing of network assets.	X
Perform network vulnerability assessments.	X
Perform network risk assessments of people, processes, technologies, and/or operations.	X
Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.	X

Table A2.4.3. Added: Computer Network Defense – Service Provider Incident Responder Position.

(Primary Focus: Personnel Assigned to Units Performing Computer Network Defense – Service Provider Missions)

Duties	Computer Network Defense – Service Provider <u>Incident Responder</u>
Collect and analyze intrusion artifacts (e.g., source code, malware, trojans).	X
Coordinate with intelligence analysts to correlate threat assessment data.	X
Correlate incident data.	X
Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation.	X
Perform network trend analysis and reporting.	X
Perform real-time incident handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks.	X
Serve as technical experts and liaisons to law enforcement personnel.	X
Track and document cyber incidents from initial detection through final resolution.	X
Use discovered data to develop mitigations/remediation to potential network incidents.	X
Write network guidance and reports on incident findings to appropriate constituencies/stakeholders.	X

Table A2.4.4. Added: Computer Network Defense – Service Provider Infrastructure Support Position.

(Primary Focus: Personnel Assigned to Units Performing Computer Network Defense – Service Provider Missions)

Duties	Computer Network Defense – Service Provider Infrastructure Support
Configure and manage alerts, indicators, rules, and/or signatures for cybersecurity applications and tools.	X
Create, edit, and manage changes to network access control lists on cybersecurity tools/systems (e.g., firewalls and intrusion prevention systems).	X
Implement alerts, indicators, rules, and/or signatures for cybersecurity applications, systems, and tools.	X
Maintain CND-SP training lab/network.	X
Perform system administration (e.g., install, configure, backup, restore) on cybersecurity applications, systems, and tools.	X
Test and evaluate cybersecurity applications/systems/tools, rules/signatures, access controls, and configurations of CND-SP managed platforms.	X
Work with Computer Network Defense - Service Provider Analyst(s) to review logs and develop mitigations.	X

Table A2.4.5. Added: Computer Network Defense – Service Provider Manager Position.

(Primary Focus: Personnel Assigned to Units Performing Computer Network Defense – Service Provider Missions)

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

Table A2.5. Added: Senior Software Development Roles - Senior Software Developer/Senior Software SME/Senior Software Tester

Duties	Senior Software Development Roles
Address security implications in the software acceptance phase for the following: completion criteria, risk acceptance & documentation, common criteria, and methods of independent testing.	X
Analyze and provide information to stakeholders that will support the development of a security application or modification of an existing security application.	X
Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	X
Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	X
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
Define testing criteria for new or updated applications.	X
Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	X
For a major weapon system, 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. DoD Instruction 5000.02 defines “major weapon system”	X
Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	X
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

Attachment 5 Changed to read:

SAMPLE - FORMAL STATEMENT OF RESPONSIBILITIES

(Applicable for Civilians and Military)

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cyber Security Responsibilities

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

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

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

3. I understand I will attain and maintain the appropriate DoD approved cybersecurity baseline certification(s) applicable for the cybersecurity functions/tasks assigned above and required for the above position IAW AFMAN 17-1303 and DoD 8570.01-M.

Member’s Name:	
Member’s Signature:	

Supervisor’s Name:	
Supervisor’s Signature:	

KEEP SIGNED DOCUMENT LOCALLY

END OF SAMPLE

Attachment 6 Changed to read:

SAMPLE FORMAL STATEMENT OF RESPONSIBILITIES

(Applicable for Contractors)

MEMORANDUM FOR RECORD

SUBJECT: Formal Statement of Assigned Cyber Security Responsibilities

1. IAW AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, Paragraph 2.20.4, I understand my contract role has a 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 **c**ontract role.

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

Contractor Name:	
Contractor Signature:	

COR/Designated Government Representative Name:	
COR/Designated Government Representative Signature:	

KEEP SIGNED DOCUMENT LOCALLY

------END OF SAMPLE----

This Memorandum will supersede AFMAN17-1303_AFGM2017-01. This Memorandum becomes void after one-year has elapsed from the date of this Memorandum, or upon publication of a rewrite of the affected publication.

WILLIAM E. MARION II, SES, DAF
Acting Chief, Information Dominance and
Acting Chief Information Officer

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-285

20 MARCH 2015

Incorporating Change 1, 26 May 2016

Communications and Information

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/CIO A6SF Force Development

Certified by: SAF/CIO A6S (Col Mary Hanson, AF SISO)

Supersedes: AFMAN33-285, 17 June 2011

Pages: 62

This Air Force Manual (AFMAN) implements Department of Defense (DoD) Directive (DoDD) 8570.01, *Information Assurance Training, Certification, and Workforce Management*; DoD 8570.01-M, *Information Assurance Workforce Improvement Program;* Air Force Policy Directive (AFPD) 33-2, *Information Assurance Program* and Air Force Instruction (AFI) 33-200, *Information Assurance Management*. This manual applies to Air Force military, civilian and contractor personnel under contract to the DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems. This publication also applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC). 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/CIO A6. Send any supplements to this publication to SAF/CIO A6 for review, coordination, and approval prior to publication. Unless otherwise noted, the SAF/CIO A6 is the waivering authority to policies contained in this publication. The authorities to waive wing/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*, Table 1.1 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 Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). 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 interim change revises AFMAN 33-285 only by (1) extending the implementation due dates of the cybersecurity (8570) certification requirement for the software developer/engineer/programmer role supporting a(n) information system (IS)/platform information technology (PIT) system and (2) updating several embedded links. A margin bar (|) indicates newly revised material.

Chapter 1

GENERAL INFORMATION

1.1. Objectives. This manual implements DoDD 8570.01, *Information Assurance (IA) Training, Certification and Workforce Management*, 15 August 2004 and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 and specifically identifies AF requirements, roles, and responsibilities. The primary objective of the Air Force (AF) Cybersecurity Workforce Improvement Program (WIP) is to train, educate, certify, and qualify personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and dispose/retire DoD Systems. All authorized users of DoD information systems (ISs)/Platform Information Technology (PIT) systems must receive initial cybersecurity user awareness training as a condition of access to an IS IAW DoD 8570.01-M, Paragraph C6.2.2.; thereafter, all users will complete annual cybersecurity awareness refresher training **(T-0)**. This training can be found on the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) portal: **http://iase.disa.mil/eta/Pages/index.aspx**. This manual also identifies AF cybersecurity workforce positions, certification and qualifications requirements, and provides policy on cybersecurity workforce reporting, metrics and validation Unless noted, the cybersecurity position requirements (e.g. certification, training, etc.) specified in this manual are the minimum required. Commanders are authorized to increase requirements to reflect specific duties and or function(s).

1.2. Goal. IAW DoD 8570.01-M, the goal of the Cybersecurity WIP is to "develop a DoD cybersecurity [IA] 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 (CIA) of DoD information, information systems, networks and information stored within." The Cybersecurity WIP provides warfighters qualified cybersecurity personnel in each category, specialty and level: Information Assurance Technical (IAT), Information Assurance Management (IAM), Computer-Network Defense - Service Providers (CND-SPs), IA System Architects and Engineers (IASAEs), Authorizing Officials (formerly called Designated Accrediting/Approving Authorities [DAAs]), and Assessing Functions.

1.3. Applicability. Cybersecurity workforce functions and associated DoD approved baseline cybersecurity certifications are identified in DoD 8570.01-M by category (IAT and IAM) or specialty (CND-SP and IASAE). The cybersecurity workforce positions on a unit manning document (UMD) will reflect the certification required using established special experience identifiers (SEIs). The cybersecurity workforce consists of all civilian, military, and contractors performing a cybersecurity function IAW DoD 8570.01-M, requires possession of a current/valid cybersecurity baseline certification, and all Airmen who are required to possess a valid/current baseline cybersecurity certifications as a precondition of their respective Air Force Specialty Code (AFSC). This manual applies to all AF civilian, military, and contractor (US citizens, Foreign Nationals [FNs], and Local Nationals [LNs]) personnel performing cybersecurity functions or tasks IAW DoD Chief Information Officer (DoD CIO) policies. AFMAN 33-285 compliance is required for the Intelligence Community (IC) and Special Access Program (SAP) unless AFMAN conflicts with the Office of Director of National Intelligence (ODNI) or the DoD Director, Special Access Programs Central Office (DoD SAPCO) directives respectfully. When in conflict, the ODNI and DoD SAPCO Guidance take precedence for the IC and SAP

community. Although DoD 8570.01-M requirements have been vetted through OSD legal channels and with National Unions, DoD CIO has strongly recommended continuous engagements with appropriate local parties such as the local or country Human Resources section of the Office of Personnel Management (OPM) or local unions.

1.3.1. For this manual, the term civilian includes AF employees (US citizens, FNs and LNs) paid by appropriated funds. The definitions for FNs and LNs can be found in DoD 8570.01-M, Appendix 1.

1.3.2. For this manual, the term military reflects the Total Force (Active Air Force, Air National Guard, and Air Force Reserve Components). Also, the term military includes US citizens and FNs.

1.3.3. For the manual, the term contractor includes US citizens, FNs, and LNs.

1.3.4. For this manual, the term major command (MAJCOM) includes field operating agency (FOA) and direct reporting unit (DRU).

1.3.5. For this manual, the term Program Management Office (PMO) is synonymous with the Program/Project Manager (PM) or System Manager. PMOs or PMO-like entities manage the acquisition, delivery, and sustainment of information technology, including ISs/PIT systems.

1.3.6. For this manual, the term IA Managerial (IAM) refers to the management category of 8570-related certifications, but is not synonymous with the Information System Security Manager **(**ISSM) (formerly called Information Assurance Manager) position.

1.3.7. For this manual, the term Base/Wing ISSM is synonymous with the Wing Cybersecurity Officer (formerly called Wing Information Assurance Officer).

1.3.8. For this manual, the term AF 8570 Program (centralized) funds refers to the budget/funds managed by AF Space Command Cyber Support Squadron (AFSPC CYSS) to pay for both cybersecurity baseline certifications exams and maintenance fees for AF civilian and military personnel.

1.4. Requirements. Commanders and supervisors will do the following: identify cybersecurity workforce positions in manpower databases/systems; ensure personnel are trained, certified, and qualified; record cybersecurity workforce information in personnel systems; track and ensure certifications are current; and report certification status **(T-0)**. DoD has agreed to adhere to certification currency requirements as stipulated by the International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17024 for the commercial cybersecurity certifications. For civilian and military personnel, the cybersecurity workforce information will be recorded in manpower and personnel databases/systems (e.g. Military Personnel Data System [MILPDS] and Defense Civilian Personnel Data System [DCPDS]), to include but not limited to, AFSC or civilian occupational series **(T-0)**. For contractors, all cybersecurity requirements, including currency, must be recorded in the contracts (new or modified)/Performance-Based Work Statement (PWS) IAW 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)**.

1.4.1. All AF workforce (civilian, military, and contractor) positions regardless of AFSC, occupational series, or job title performing one or more cybersecurity functions must be

identified, managed, and tracked as part of the DoD cybersecurity workforce IAW DoD 8570.01-M, Paragraph C1.4.4.7 **(T-0)**. Individuals occupying these positions will attain and maintain a DoD approved cybersecurity baseline certification(s) as outlined in DoD 8570.01-M, Paragraph AP2.1.2.1 **(T-0)**. Also, all AF cybersecurity workforce personnel will become qualified in assigned cybersecurity position IAW DoD 8570.01-M, Paragraph C2.3.6 **(T-0)**. Please see the AF Cybersecurity Position Certification Determination Guide, Attachment 2, for further guidance on certification requirements.

1.4.2. All AF positions involved in the performance of cybersecurity functions must be identified in manpower and personnel databases/systems **(T-0)**.

1.4.3. AF supervisors should have the capability to identify, manage, and track personnel performing cybersecurity functions, regardless of military specialty or occupational series.

1.4.4. The status of cybersecurity qualifications must be monitored and tracked IAW DoD 8570.01-M, Paragraph C8.1.1 **(T-0)**.

1.5. Background. The AF recognizes the following agencies must provide support as listed in DoD 8570.01-M: (1) The DoD CIO will provide overarching cybersecurity policy and guidance and coordinate the implementation and sustainment requirements of DoD 8570.01-M to include supporting tools and resources (e.g., conferences, websites, database integration, workforce identification, etc.); (2) The Under Secretary of Defense for Personnel and Readiness (USD [P&R]) will support and provide appropriate representation to the USD (P&R) Cybersecurity Training, Certification, and Workforce Management Oversight Advisory Council; and (3) The Director of DISA will coordinate with the Defense-wide Information Assurance Program office and the components to develop and maintain online resources correlating DoD cybersecurity training products and classes.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Air Force Chief of Information Dominance and Chief Information Officer (SAF/CIO A6).

2.1.1. Develop policy and direct implementation of AF requirements and processes. Interpret and promulgate cybersecurity workforce directives, policies and requirements such as DoD 8570.01-M.

2.1.1.1. Provide direction on position determinations for the cybersecurity workforce.

2.1.1.2. Provide direction and 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 of the cybersecurity workforce.

2.1.1.4. Provide programming and budget guidance to Core Function Leads (CFLs) and MAJCOMs for cybersecurity workforce management and improvement programs to include certification exam and maintenance fee costs, and computer-based training.

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

2.1.1.6. Provide direction on supplemental cybersecurity workforce training.

2.1.2. Oversee Cybersecurity WIP and distribution of certification funds for the AF.

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

2.1.4. Collect and report on qualification metrics and submit reports to the DoD CIO as directed such as for Federal Information Security Management Act (FISMA) reporting, standardizing reporting across Air Force.

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. Certify and Accredit the software needed by the education offices using .mil).

2.1.8. Coordinate with SAF/A1 to integrate 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. *Note*: Career field specific requirements are coordinated with the respective career field manager for integration into Career Field Training Plan (CFETP)/Specialty Training Standard (STS)/Course Training Standard (CTS) as appropriate.

2.1.9. Acquire capability for PMOs/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 AETC has the most current DoD approved with annual cybersecurity user awareness training product(s).

2.1.12. Work with SAF/A1 and SAF/AQ on a capability to automate reporting of the qualification status of the AF cybersecurity workforce.

2.2. Assistant Secretary of the Air Force, Acquisition (SAF/AQ).

2.2.1. Ensure ISs/PIT systems acquisitions address cybersecurity workforce requirements.

2.2.2. Ensure programs budget for certified and qualified cybersecurity support for certified and qualified personnel throughout system life cycles.

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

2.3.1. Provide a capability to identify, record and track civilian and military cybersecurity positions via SEIs on the UMD IAW DoD Instructions, DoD 8570.01-M, and AF policies.

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/systems.

2.4. MAJCOMs/FOAs/DRUs.

2.4.1. Ensure cybersecurity workforce is identified, trained, certified, qualified, tracked, and managed IAW DoD and AF cybersecurity WIP directives and policies such as DoDD 8570.01, DoD 8570.01-M, and this manual.

2.4.2. Ensure the cybersecurity workforce positions are reviewed periodically and validated annually. SAF/CIO A6 will provide the reporting instructions for validations.

2.4.3. Appoint MAJCOM/FOA/DRU Cybersecurity WIP representatives to SAF/CIO A6. This individual should brief MAJCOM/A6 on implementation issues.

2.4.4. Act as the command focal point (or equivalent) and provide MAJCOM guidance and oversight for DoD 8570.01-M issues.

2.4.5. Consolidate base/wing reporting inputs on civilian, military, and contractor cyberspace workforce requirements.

2.4.6. Provide AFSPC CYSS contact information for POCs.

2.4.7. Report the status of their cybersecurity workforce (civilian, military, and contractors) qualifications to the SAF/CIO A6 IAW **Paragraph 7.2**.

2.4.8. Report on annual validation of civilian and military cybersecurity workforce positions to the SAF/CIO A6 IAW **Paragraph 7.3**.

2.5. Headquarters Air Education and Training Command (HQ AETC).

2.5.1. Provide and sustain availability of cybersecurity user awareness training provided by the SAF/CIO A6.

2.5.2. Provide schoolhouse training, certification testing, and cybersecurity user awareness training to students as appropriate.

2.6. Air Force Personnel Operations Agency (AFPOA).

2.6.1. Extract reports from manpower and personnel databases/systems (e.g. MILPDS and DCPDS) to identify cybersecurity workforce certification requirements and certified personnel for AF compliance reporting.

2.6.2. Provide technical assistance to the SAF/CIO A6 on manpower and personnel systems such as data field entries.

2.7. Air Force Personnel Center (AFPC).

2.7.1. Upon the request of the appropriate SAF/CIO A6 Career Field Manager (CFM), update the Air Force Enlisted Classification Directory (AFECD) and/or AF Officer Classification Directory (AFOCD) with SEIs to track the military cybersecurity workforce.

2.7.2. Validate cybersecurity certification completion for civilian personnel in civilian personnel database(s)/system(s).

2.7.3. Validate cybersecurity certification completion for military personnel in military personnel database(s)/system(s).

2.8. Air Force Space Command (AFSPC).

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

2.8.2. Submit Program Objective Memorandum (POM) 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 program.

2.8.5. Publish information regarding AF-endorsed certification requirements.

2.8.6. Execute AF centralized funds for preferred certifications and maintenance fees.

2.9. Director of Security, Special Programs Oversight (SAF/AAZ). Ensure SAP information systems and platform information technologies compliance with cybersecurity/IA workforce requirements with certified and qualified personnel throughout system and platform life cycles.

2.10. Authorizing Officials (AO).

2.10.1. Comply with cybersecurity training requirements IAW **Paragraph 3.2.4**. The AO training is located on the DISA IASE portal: **http://iase.disa.mil/eta/Pages/index.aspx**.

2.10.2. Provide oversight over cybersecurity personnel and positions, supporting responsible ISs/PIT systems IAW **Paragraph 3.2.11**.

2.10.3. Provide oversight over the cybersecurity baseline certification waiver process IAW C**hapter 8**. These waivers must be only applicable to cybersecurity-related positions under the AO's authority.

2.11. Air Force Career Field Manager(s) (AF CFMs).

2.11.1. Periodically review AFSC(s) or occupational series and certification level for inclusion/removal in the cybersecurity workforce program.

2.11.2. Ensure enlisted and officer classification directories are updated with SEIs for tracking cybersecurity workforce requirements or certifications for the AFSC(s) the CFM manages.

2.11.3. Ensure civilian position description (PD) guidance is provided for tracking cybersecurity workforce requirements or certifications for applicable occupational series.

2.12. MAJCOM/FOA/DRU WIP Representative(s).

2.12.1. Ensure cybersecurity workforce requirements in DoDD 8570.01 and DoD 8570.01-M are met.

2.12.2. Provide oversight over the qualification status (e.g. training, certification, continuing education, etc.) for all personnel identified as part of the AF cybersecurity workforce.

2.12.3. Ensure qualification status of AF cybersecurity workforce is tracked and reported as an element of mission readiness and as a management review item.

2.12.4. Provide cybersecurity workforce compliance statistical data in appropriate format to the SAF/CIO A6 IAW **Paragraph 7.2**.

2.13. Wing Cybersecurity Office (WCO, formerly called Wing Information Assurance Office).

2.13.1. Will monitor status of AF cybersecurity workforce including certification, training, and qualifications criteria (e.g. on-the-job evaluation [OJE], continuing education, and personnel security investigation [e.g. National Agency Check [NAC], NAC plus Written Inquiries, Background Investigation, Single Scope Background Investigation [SSBI]]) **(T-1)**.

2.13.2. Provide oversight over the Privileged Access Agreement process of cybersecurity workforce (civilians, military and contractors) within their wing/base.

2.13.3. Will report statistics on Wing's cybersecurity workforce personnel compliance IAW this manual to the MAJCOM/FOA/DRU WIP Representative(s) as an element of mission readiness and as a management review item **(T-1)**.

2.14. Information System Security Managers (ISSMs).

2.14.1. Will develop a process to validate an individual has signed a Privileged Access Agreement, completed the appropriate clearance or personnel security investigation appropriate for access, and cybersecurity baseline certification(s) before privileged access to IS/PIT system is granted **(T-2).**

2.14.2. Will track Privileged Access Agreements for each responsible ISs/PIT system **(T-2)**. Provide updates to the WCO.

2.14.3. Will ensure the ISs/PIT system cybersecurity workforce certification and training meets compliance for mission readiness and management review items **(T-2)**.

2.15. Civilian Personnel Section (CPS).

2.15.1. Will process personnel action request(s) such as Authorization Change Request (ACRs) to identify cybersecurity workforce requirements within appropriate personnel database(s)/system(s) **(T-2)**.

2.15.2. 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 (CPD) and position classification **(T-2)**.

2.15.3. Ensure the Labor Relations Officer confirms collective bargaining obligations are met.

2.16. Program/Project Managers (PMs), System Managers (SMs), Program Management Offices (PMOs), Developmental/Operational Test Agencies, and Units.

2.16.1. Will enforce tracking and management of their cybersecurity workforce (civilian, military, and contractor) personnel, ensuring personnel are certified and qualified IAW DoD 8570.01-M and this manual **(T-0)**.

2.16.2. Will review the UMD to ensure all civilian and military cybersecurity-related positions are identified and recorded positions 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)**.

2.16.3. Will ensure personnel in cybersecurity workforce positions possess the appropriate clearance or personnel security investigation for position IAW DoD 8570.01-M, Paragraph C1.4.4.6.4 **(T-0)**.

2.16.3.1. Will not approve/initiate privileged access requests for an IS/PIT system until individual possesses the appropriate the clearance or personnel security investigation **(T-0)**.

2.16.4. Will ensure civilian CPDs/PDs reflect accurately cybersecurity workforce requirements **(T-0)**.

2.16.5. Will identify organization's civilian positions in the cybersecurity workforce IAW DoD 8570.01-M, Paragraph C7.3.2.2 **(T-0)**.

2.16.6. Will ensure servicing CPS and position classification functions are notified of any changes to civilian positions in the cybersecurity workforce **(T-2)**.

2.16.7. Will provide corrective actions, when necessary, to implement the requirements within this manual **(T-2)**.

2.16.8. Will ensure contractor cybersecurity workforce requirements and compliance are managed through the contract process **(T-0)**.

2.16.8.1. Will ensure contractor personnel, IAW DoD 8570.01-M, Paragraph C2.3.9, have appropriate DoD approved cybersecurity baseline certification(s) prior to supporting any cybersecurity functions for new or recently modified contracts **(T-0)**.

2.16.8.2. , Will ensure, IAW DoD 8570.01-M, Paragraphs C1.4.4.5, all contracts (new or modified) and PWSs must state all cybersecurity requirements, including baseline certification category/specialty and level, for contractor personnel **(T-0)**. The PWS

should state the following: "The contractors will comply with the Defense Acquisition Regulations (DFARS) 252.239.7001 and all cybersecurity requirements stipulated in the contract..."

2.16.8.3. The Contracting Officer (CO) will ensure, IAW DoD 8570.01-M, Paragraph C2.3.9, all contractor personnel are appropriately certified **(T-0)**. For instance, the CO will validate all newly assigned contractors have the appropriate certification(s) prior to being given privileged access to the network and/or assuming cybersecurity responsibilities **(T-0)**.

2.16.8.4. Will ensure all contractor personnel complete/sign a formal statement of assigned cybersecurity responsibilities **(T-0)**. A suggested format can be found in **Appendix 6** for contactors.

2.16.8.5. Contractor personnel who are required to have a cybersecurity baseline certification and do not maintain the certification(s), in good standing, will be immediately removed from task **(T-0)**. Contractors are ineligible for certification baseline waivers as described in **Chapter 8**. Coordinate with the servicing contracting office regarding removal process **(T-0)**.

2.16.9. Will only assign US citizens to IA Workforce Technical (IAT) Category Level III, IA Workforce Management (IAM) Category Level III, and IA Workforce System Architect and Engineer Specialty Level III positions IAW DoD 8570.01-M, Tables C3.T6, C4.T6, and C10.T6 **(T-0)**.

2.16.10. Will take appropriate actions IAW **Paragraph 5.6** on civilian and military personnel in cybersecurity workforce positions when cybersecurity baseline certifications are not achieved within six months of filling the position, baseline certification waivers (see **Chapter 8**) are not obtained, an individual has become decertified, or a baseline certification has expired **(T-0)**.

2.16.11. Will budget for training and re-testing for individuals who fail their certification exam; for individuals who will be re-certificated due to failure of maintaining baseline certification in good standing; and for those individuals who desire training over and above the training resources provided by SAF/CIO A6 or AFSPC CYSS **(T-3)**.

2.16.12. Will not initiate certification waivers for contractors IAW DoD 8570.01-M, Paragraphs C2.3.9 **(T-0)**.

2.16.13. Will report the status of their cybersecurity workforce (civilian, military, and contractors) qualifications to the SAF/CIO A6 IAW **Paragraph 7.2 (T-0)**.

2.16.14. Will conduct annual validation of civilian and military cybersecurity workforce positions **(T-0)**.

2.16.15. Will provide update on cybersecurity workforce qualifications statistics to the local WCO **(T-0)**.

2.17. Unit Training Managers (UTM).

2.17.1. Will initiate and coordinate AF Form 2096(s) for commander approval (with further submission to servicing personnel function (Force Support Squadron [FSS], Military

Personnel Flight [MPF], or equivalent), to award SEI for military cybersecurity members achieving certification **(T-3)**.

2.17.2. Will plan and organize required cybersecurity training and certification for the organization's civilian and military cybersecurity workforce **(T-3)**.

2.17.3. Will track, monitor, and document the progress of the baseline training, continuing education (CE) units, and Computing Environment/Operating System training for the organization's civilian and military cybersecurity workforce **(T-3)**.

2.17.4. Will ensure every civilian, military, and contractor in the organization/unit has authorized release of their cybersecurity baseline certification to the Defense Manpower Data Center (DMDC) IAW DoD 8570.01-M, Paragraph C2.3.12 **(T-0)**. The authorization release can be found at this link: **https://www.dmdc.osd.mil/appj/dwc/index.jsp.** The UTM should engage applicable MAJCOM/FOA/DRU WIP Representative(s) for latest info on released cybersecurity baseline certifications.

2.18. Supervisors.

2.18.1. Will incorporate cybersecurity certification and qualification requirements IAW **Chapter 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 attain and maintain qualifications **(T-3)**.

2.18.3. Will ensure civilians and military complete/sign a formal statement of assigned cybersecurity responsibilities **(T-0)**. A suggested format can be in Appendix 5 for civilians and military.

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

2.18.5. Will approve certification exam requests for eligible civilian and military personnel in coded cybersecurity workforce positions with at least one year retainability **(T-0)**.

2.18.6. Will validate personnel (civilian and military) have completed, if applicable, the appropriate computing environment/operating system training IAW **Paragraph 4.2** for assigned duties **(T-0)**.

2.19. Individuals (Civilian and Military).

2.19.1. Will attain appropriate DoD approved cybersecurity baseline certification(s) applicable for cybersecurity functions required for the DoD position held, within six months of filling position IAW 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 in good standing cybersecurity baseline certification(s) IAW 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.

2.19.3. 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 IAW DoD 8570.01-M, Paragraphs C3.2.4.4, C4.2.3.6, and C10.2.3.6 **(T-0)**.

2.19.5. Will sign Privileged Access Agreement if privileged access is required, for each IS/PIT system necessary to perform assigned duties IAW 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 cybersecurity baseline certification data to DoD via DMDC IAW DoD 8570.01-M, Paragraphs C2.3.12 **(T-0)**. The authorization release can be found at: **https://www.dmdc.osd.mil/appj/dwc/index.jsp**.

2.19.7. Will report Continuing Education Units (CEUs) status to supervisor and UTM **(T-0)**.

2.20. Individuals (Contractors).

2.20.1. Will attain appropriate cybersecurity certification(s) applicable for assigned cybersecurity workforce position prior to start of contractual duties IAW DoD 8570.01-M, Paragraph C2.3.9 **(T-0)**.

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

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

2.20.4. Will sign a formal statement of assigned cybersecurity responsibilities IAW 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 the Privileged Access Agreement if privileged access is required, for each IS/PIT system necessary to perform assigned duties IAW 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 the release of cybersecurity baseline certification data to DMDC IAW DoD 8570.01-M, Paragraphs C2.3.12 **(T-0)**. The authorization release can be found at: **https://www.dmdc.osd.mil/appj/dwc/index.jsp.**

2.20.7. Will not be eligible for cybersecurity baseline certification waivers IAW 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 statements of work to determine if cybersecurity functions are required to be performed by that position IAW DoD 8570.01-M, **Chapter 3**, 4, 5, 10, and 11 **(T-0)**. Please refer to the AF Cybersecurity Position Certification Determination Guide, **Attachment 2**, to assist supervisors and managers in the identification process. If a position is identified as part of the cybersecurity workforce, then the requirement must be recorded and, if encumbered, the assigned individual will achieve the appropriate certification commensurate with the position **(T-0)**. If a position is performing functions spanning across one or more levels within a category/specialty, then the position certification requirements must be those of the highest level function(s) IAW DoD 8570.01-M, Paragraph C2.2.5 **(T-0)**. Supervisors should try to consolidate positions performing cybersecurity functions as an additional duty (performing functions 15 to 24 hours weekly) or an embedded duty (performing functions up to 14 hours weekly) maximizing resources. Likewise, supervisors should try to limit number of individuals requiring privileged access to the minimum necessary to support mission tasks.

3.2. Cybersecurity Workforce. The AF cybersecurity workforce is grouped by categories IA (IAT and IAM) or specialties (CND-SP and IASAE). The categories and specialties are subdivided further into levels, related to functional skill requirements and/or system environment focus. Civilians and military personnel will attain a DoD approved cybersecurity baseline within six months of formal assignment of cybersecurity duties, except as noted in **Paragraph 3.2.8** for software developers/engineer/programmers, and IAW DoD 8570.01-M, Paragraph C3.2.4.1.1 **(T-0)**. The list of DoD approved cybersecurity baseline certifications can be found at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx**. Please note the AO position does not have a mandatory cybersecurity baseline certification.

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

3.2.1.1. IAT Level I. An IAT Level I position ensures client-level workstations or end user devices (i.e. mobile device, laptop, etc.) are more secure by correcting anomalies/vulnerabilities and/or implementing security controls in the hardware or software installed. This environment usually consists of a client-level workstation/end user device, its operating system, peripherals, and applications. An individual in an IAT Level I position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. Examples of IAT Level I could include a Client Support Technician having root access/rights to the operating system at the workstation or end user device and help desk support staff.

3.2.1.2. IAT Level II. An IAT Level II position provides networked environment (NE) support. For this manual, networked is defined as two or more workstations or ISs/PIT systems interconnected. Also, the IAT Level II pays special attention to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. An individual in an IAT II position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. Examples of IAT Level II could include technician of internetworking devices such as routers and switches, personnel supporting cabling infrastructures, and system administrators for networked, but non-enterprise (i.e. not accessible to global end users) servers.

3.2.1.3. IAT Level III. An IAT Level III position is responsible for incident response and making local technical decisions regarding the cybersecurity posture of the enterprise asset. An individual in an IAT III position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. An example of IAT Level III could include a Security Control Assessor Representative (formerly called Certifying Authority Representative) who performs mostly technical assessments/audits and an individual responsible for the overall administration of enterprise-level network devices/servers/services.

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

3.2.2.1. IAM Level I. An individual in an IAM Level I position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. Examples of an IAM Level I could include crew commanders and WCO staff, except for the Base/Wing ISSM.

3.2.2.2. IAM Level II. An individual in an IAM Level II position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. An Example of an IAM Level II is the Base/Wing ISSM.

3.2.2.3. IAM Level III. An individual in an IAM Level III position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 **(T-0)**. Examples of an IAM Level III could include the AF Senior Information

Security Officer (AF SISO), SAF/CIO A6 cybersecurity staff personnel, several MAJCOM cybersecurity staff positions, Security Control Assessor (SCA), and ISSM for IS(s)/PIT system(s) providing enterprise capabilities and/or services to AF end users worldwide **(T-1)**.

3.2.3. AF Senior Information Security Officer (SISO). The AF SISO is the official responsible for directing the Air Force's cybersecurity program on behalf of the AF CIO. The AF SISO will attain and maintain an IAM Level III cybersecurity baseline certification. It is recommended the AF SISO attain other certifications. AF centralized funds will pay for cybersecurity baseline certification exam and maintenance fees **(T-1)**.

3.2.4. Authorizing Official (AO). The AO is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. IAW DoD 8570.01-M, Paragraph C5.3.11, the AO will complete a DoD mandated AO training module within 60 days of assignment **(T-0)**.

3.2.5. Assessment Functions.

3.2.5.1. Security Control Assessor (SCA). The SCA (formerly called Certifying Authority [CA]) is the senior official having the authority and responsibility for the assessment of an IS/ PIT system. The SCA roles and responsibilities are addressed in AFI 33-210. SCAs will attain and maintain a DoD approved IAM Level III cybersecurity baseline certification **(T-1)**. Also, it is highly recommended SCAs should both complete the AO training module and attain the Committee on National Security Systems Instruction (CNSSI) 4016 certificate, for supplemental training on the AO responsibilities and risk analysis/mitigation, respectively.

3.2.5.2. Security Control Assessor Representative (SCAR). SCARs will attain and maintain a DOD approved Level III cybersecurity baseline certification commensurate to assigned position **(T-1)**. The SCAR position will be classified as either IAM Level III or IAT Level III. The AO can designate the SCAR as an IAT Level III position, if the SCAR is performing predominately technical assessment/validation of security controls. Otherwise, the AO can designate the SCAR as an IAM Level III position. Also, it is highly recommended SCARs should complete the AO training module and attain the CNSSI 4016 certificate or supplemental training on the AO responsibilities and risk analysis/mitigation, respectively.

3.2.6. IA System Architect and Engineer (IASAE) Specialty.

3.2.6.1. IASAE Level I. An IASAE Level I position is responsible for the design, development, implementation, and/or integration of a DoD IS/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 IS/PIT system. An individual in an IASAE Level I position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 **(T-0)**.

3.2.6.2. IASAE Level II. An IASAE Level II position is responsible for the design, development, implementation, and/or integration of a DoD cybersecurity architecture,

system, or system component for use within the Network Environment (NE). For this manual, networked is defined as two or more ISs/PIT systems, workstations and/or end user devices directly interconnected, but where the adverse impacts can be localized/isolated only to those interconnected. Examples could include ISSEs supporting functional-level systems connected to the DoDIN, but where adverse impacts can be isolated to only those who are interconnected. An individual in an IASAE Level II position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 **(T-0)**.

3.2.6.3. IASAE Level III. An IASAE Level III position is responsible for the design, development, implementation, and/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 IS(s)/PIT system(s) are operational and secure. Examples include ISSEs supporting enterprise-level (irrespective of functional community) IS(s) connected to the DoDIN. An individual in an IASAE Level III position will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 **(T-0)**.

3.2.7. Computer Network Defense – Service Provider (CND-SP) Specialty Positions. These positions are located within organization(s) providing cybersecurity provider functions.

3.2.7.1. CND-SP Analyst (CND-A). A CND-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 CND-A position will attain and maintain both an IAT cybersecurity baseline certification **and** a CND baseline certification commensurate assigned position from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 and Table C 11.T2 **(T-0)**.

3.2.7.2. CND-SP Infrastructure Support (CND-IS). A CND-IS tests, implements, deploys, maintains, and administers the infrastructure assets/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/prevention systems. An individual in a CND-IS position will attain and maintain both an IAT cybersecurity baseline certification commensurate to assigned level **and** a CND baseline certification commensurate to assigned position from the DoD approved listing located at: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 and Table C 11.T4 **(T-0)**.

3.2.7.3. CND-SP Incident Responder (CND-IR). A CND-IR investigates and analyzes all response activities related to cyber incidents. An individual in a CND-IR position will attain and maintain both an IAT cybersecurity baseline certification to assigned level **and** a CND baseline certification commensurate to assigned position from the DoD approved

listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 and Table C 11.T6 **(T-0)**.

3.2.7.4. CND-SP Auditor (CND-AU). A CND-AU performs assessments of systems and networks within the NE or enclave and identify where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. An individual in a CND-AU position will attain and maintain both an IAT cybersecurity baseline certification **and** a CND baseline certification commensurate to assigned position from the DoD approved listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraph C2.3.2 and Table C11.T8 **(T-0)**.

3.2.7.5. CND-SP Manager (CND-SPM). A CND-SPM oversees the cybersecurity service provider functions. A CND-SPM is responsible for producing guidance, assisting with risk assessments and risk management, and managing the technical classification. An individual in a CND-SPM position will attain and maintain both an IAM cybersecurity baseline certification **and** a CND baseline certification commensurate to assigned position from the DoD approved listing located at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx** IAW DoD 8570.01-M, Paragraphs C2.3.2 and Table C11.T10 **(T-0)**.

3.2.8. Information System Security Managers (ISSMs) for IS/PIT System. An ISSM for an IS/PIT system creates and/or oversees the cybersecurity program to include cybersecurity architecture, requirements, personnel, policies, processes and procedures. The ISSM acts as the primary cybersecurity technical advisor to the AO. As such, it is imperative that the ISSM have the appropriate foundational knowledge of cybersecurity best practices and risk management commensurate to the criticality of information stored and/or processed on the ISs/PIT systems. For ISs/PIT systems providing enterprise capabilities and/or services to AF end users worldwide, the ISSM will attain and maintain, at a minimum, an IAM Level III cybersecurity baseline certification **(T-1)**. For ISs/PIT systems that are networked and interconnected, but do not provide enterprise capabilities and/or services to AF end users worldwide, the ISSM will attain and maintain, at a minimum, an IAM Level II cybersecurity baseline certification **(T-1)**. Roles and responsibilities of ISSMs are addressed in AFI 33-200 and AFI 33-210.

3.2.9. Information System Security Officers (ISSOs). Roles and responsibilities of ISSOs are addressed in AFI 33-200 and AFI 33-210. For ISs/PIT systems providing enterprise capabilities and/or services to AF end users worldwide, the ISSO will attain and maintain an IAT Level III cybersecurity baseline certification **(T-1)**. Otherwise, the ISSO position will attain and maintain, at a minimum, an IAT Level II cybersecurity baseline certification **(T-1)**.

3.2.10. Privileged Access Users. Every privileged user will be assigned to a cybersecurity-coded position on the UMD. Also, every privileged user will attain and maintain a cybersecurity baseline certification commensurate to the category and level from the DoD approved listing. The CNSSI 4009 defines a "privileged user" as a user that is authorized (and, therefore, trusted) to have elevated rights to perform security-relevant functions that ordinary users are not authorized to perform. IAW DoD 8570.01-M, Paragraph AP1.22**,** an individual who has access to system control, monitoring/security, administration, criminal investigation or compliance functions to an IS/PIT system must be classified as an AF "privileged user," except for exemption specified in **Paragraph 3.2.11 (T-1)**.

3.2.11. Cybersecurity Baseline Certification Requirement Exemption Process for Individuals Supporting IS/ PIT System. Cybersecurity is critical for ensuring information is protected and IS/PIT system meets 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-approved publications (e.g. Technical Orders, aids, software handbooks, checklists and contractor-developed technical manual procedures) to facilitate operation, troubleshooting and repair of IS/PIT system. These tasks may not require additional training, certifications, or qualifications beyond the requirements established in publications such as Mission Design Series (MDS) 11 documents and Technical Orders. The AF-approved publications have been vetted and approved by the responsible AO to prevent the unauthorized alteration of IS/PIT system cybersecurity posture. An AO can make a certification requirement determination, exempting individuals who have limited elevated network/system permissions to an IS/PIT system. The determination must apply only to IS/PIT system(s) under the AO's authority and responsibility for risk acceptance. The exemption determination memos must be initiated by Program Managers, signed by the ISSM, and routed to MAJCOM and AO for in-turn signatures**.**

3.2.11.1. The exemption determination memo:

3.2.11.1.1. Provide a general description of specific IS/PIT system.

3.2.11.1.2. Provide details on specific positions, including AFSCs/occupational series to be exempted.

3.2.11.1.3. Provide rationale why a cybersecurity baseline certification is not required.

3.2.11.1.3.1. Include details on specific actions to be performed as required by AF-approved publications with limited elevated permissions.

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

3.2.11.1.4. Annotate AO has vetted and accepted risk as described in AF-approved publications.

3.2.11.1.5. Identify process on how exempted personnel will be vetted initially and annually.

3.2.11.1.6. Provide details on the specialized training and recurrence of exempted individuals. For example, personnel have to be recertified every X months on checklist procedures by 7-level evaluator or technician.

3.2.11.1.7. Include a statement that exempted individuals sign a user agreement, stipulating the authorized actions/procedures to be performed.

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 SISO for the affected specific IS/PIT system.

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

3.2.11.4. Exempted individuals will be classified as an "Authorized User" **(T-1)**. The AF SISO, for the affected IS/PIT system, will provide the instructions to request network/system account via DD Form 2875 process for these individuals.

3.2.11.5. The PMO must complete and document in memo format an annual (i.e. occurring on anniversary date of exemption approval) validation of exemption memo to include personnel and IS/PIT system **(T-1)**. The ISSM will sign the memo and route to the MAJCOM and AO for in-turn signatures **(T-2)**. PMOs 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 SISO of the affected IS/PIT system **(T-1)**.

3.2.12. Software Developer/Engineer/Programmer Supporting IS/PIT System. A software developer/engineer/programmer designs, creates, integrates, and/or maintains customized software and database application(s) for use on Air Force networks/systems. It is critical cybersecurity is integrated into the development, sustainment and disposal of AF data, networks and systems. DoD is working to transform the skills and knowledge of its software developers/engineers/programmers, striving for a more qualified workforce, using the Defense Cyberspace Workforce Framework (still in development) and US Cyber Command Joint Cyberspace Training and Certification Standards (JCT&CS) unclassified version. To facilitate this transformation with the AF, PMOs/units must ensure the following actions are accomplished to track and manage software developer/engineer/programmer that support an IS /PIT system by the specified timelines **(T-1)**:

3.2.12.1. By 1 October 2017, PMOs/units must have completed identifying and recording civilian and military positions on UMD and personnel database(s)/system(s) **(T-1)**. SAF/CIO A6 will provide the amplifying instructions to identify and record positions.

3.2.12.1.1. The PMOs/units must identify and record all software developer/engineer/programmer positions requiring less than 4 years' experience as an IASAE Level I **(T-1)**.

3.2.12.1.2. The PMOs/units must identify and record software developer/engineer/programmer positions requiring 4 years or more experience as an IASAE Level II **(T-1)**.

3.2.12.2. By 1 April 2018, PMOs/units must have at a minimum 33% of assigned civilian and military positions filled by individuals possessing a cybersecurity baseline certification on the DoD approved listing. Also, the DoD approved certification must cover knowledge areas, in sufficient detail, 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). The knowledge areas must include, but not limited to secure software requirements and design, secure coding techniques, and secure software deployment strategies) **(T-1)**.

3.2.12.3. Effective 1 April 2018, all new contracts, modified contracts, and contracts beginning with a new option year must include the following certification requirement for any contractor software developer/engineer/programmer position supporting IS or PIT system **(T-1)**:

3.2.12.3.1. Individuals will possess a DoD approved cybersecurity baseline certification commensurate to category and level of the assigned position **(T-1)**. The DoD approved listing can be found at this link: **http://iase.disa.mil/iawip/Pages/iabaseline.aspx**.

3.2.12.3.2. The DoD approved certification, also, must cover knowledge areas in the secure software development life cycle (e.g. secure software requirements and design, secure coding techniques, and secure software deployment strategies) **(T-1)**.

3.2.12.4. By 1 October 2018, PMO/unit must have all assigned civilian and military positions filled by individuals possessing a DoD approved cybersecurity baseline certification **(T-0)**. Also, the DoD approved certification must cover knowledge areas, in sufficient detail, in the secure software development life cycle (e.g. secure software requirements and design, secure coding techniques, and secure software deployment strategies) **(T-1)**.

3.2.12.5. This mandate does not apply to software developer/engineer/programmer positions that do not support either an IS/PIT system. Also, this mandate does not include web site administrators such as SharePoint or others who incorporate pre-built modules in their organizational web sites.

3.2.13. Wing Cybersecurity Office (WCO).

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

3.2.13.2. Communications Security (COMSEC). If an individual (civilian, military, or contractor) is managing COMSEC account(s) with Key Management Infrastructure (KMI) capabilities, then that individual will attain and maintain at a minimum, an IAM Level I cybersecurity baseline certification. If an individual (civilian, military or contractor) is managing COMSEC accounts that do not have any KMI capabilities, then a baseline certification is not needed **(T-1)**.

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

3.2.14. Cybersecurity Liaison (formerly called Organizational/Unit Information Assurance Officer). There are no inherent certification/training requirements for the cybersecurity liaison position. Training is the responsibility of leadership and must be managed based upon the specific positional duties. If the position is performing one or more cybersecurity functions as described in **Attachment 2**, then the cybersecurity liaison will attain and maintain a cybersecurity baseline certification from the DoD approved listing, commensurate to the category and level of the highest level function performed **(T-3)**.

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 IAW DoD 8570.01-M, Paragraph

C7.1.4 **(T-0)**. Likewise, contractor positions must be annotated in contracts/performance work statement if performing cybersecurity functions as a primary, additional, or embedded duty **(T-1)**. It is strongly recommended to minimize the number of additional or embedded positions by consolidating workload into fewer positions.

3.3.1. Primary Duty. A cybersecurity position with primary duties focused on cybersecurity functions. The position may have other duties assigned, but the main effort focuses on cybersecurity functions. 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 functions, but in which cybersecurity functions are not the primary responsibility. On average, the position performs 15 to 24 hours weekly devoted to cybersecurity functions.

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

3.4. Recording the Cybersecurity Workforce Position Requirement. The cybersecurity workforce certification requirements (e.g. category/specialty, certification level, background/security clearance investigation) must be recorded IAW 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 CPD/PD, on the UMD, and within civilian personnel database(s)/system(s) like DCPDS **(T-0)**.

3.4.1.1. The PMOs/units must submit a signed personnel action request like the ACR to servicing manpower organization for action **(T-3)**. ACR is a tool used to propose changes to the organization/PMO/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 personnel action requests **(T-2)**: Personnel Accounting Symbol; SEI; Manpower Position Control Number (MPCN); Civilian Position Control Number (CPCN); cybersecurity category; cybersecurity level; identify whether it is a primary, additional, or embedded duty; and annotate "INFOSEC" as the position specialty **(T-1)**.

3.4.1.2. The PMOs/units must use SEIs to record cybersecurity training and experience requirements on the UMD. 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/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/unit must use the SEIs listed in **Table 3.2** **(T-1)**.

Table 3.1. Civilian SEIs (Positions Coded with Equivalent Enlisted AFSCs).

Certification Level	Civilian SEIs for Positions Coded with an Enlisted AFSC
IAT Level I	260
IAT Level II	264
IAT Level III	265
IAM Level I	266
IAM Level II	267
IAM Level III	268
CND-SP Analyst	872
CND-SP Infrastructure Support	873
CND-SP Incident Responder	874
CND-SP Auditor	875
CND-SP Manager	876
IASAE Level I	See ***Note***
IASAE Level II	See ***Not***e
IASAE Level III	See ***Note***
Note: SAF/CIO A6 is coordinating SEIs for these categories. Once established, SAF/CIO A6 will distribute to PMOs/units.	

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

Certification Level	Civilian SEIs for Positions Coded with an Officer AFSC
IAT Level I	C61
IAT Level II	C62
IAT Level III	C63
IAM Level I	C0I
IAM Level II	C0J
IAM Level III	C0K
CND-SP Analyst	See ***Note***
CND-SP Infrastructure Support	See ***Note***
CND-SP Incident Responder	See ***Note***
CND-SP Auditor	See ***Note***
CND-SP Manager	See ***Note***
IASAE Level I	See ***Note***
IASAE Level II	See ***Note***
IASAE Level III	See ***Note***
Note: SAF/CIO A6 is coordinating SEIs for these categories. Once established, SAF/CIO A6 will distribute to PMOs/ units.	

3.4.1.3. PMOs/units must coordinate CPD/PD changes with the servicing personnel function (FSS, MPF, or equivalent), servicing CPS (including the Labor Relations Officer), and civilian classification, IAW local processes **(T-1)**.

3.4.1.4. PMOs/units must submit a signed personnel action request like the ACR to the servicing civilian personnel section for further action by civilian classification to update the civilian personnel database(s)/system(s) such as (DCPDS) **(T-1)**. At a minimum, the following information must be provided on personnel action requests: MPCN; CPCN; cybersecurity category/specialty; cybersecurity level (Level I, II, or III); identify whether it is a primary, additional, or embedded duty; and annotate "INFOSEC" as the position specialty **(T-1)**.

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

3.4.2.1. The PMO/unit must submit a personnel/manpower change request like an ACR to the servicing personnel function (FSS, MPF, or equivalent) to include MPCN and valid SEIs **(T-1)**.

3.4.2.2. The AFECD has the current list of enlisted SEIs and is located on the myPers portal: **https://gum-crm.csd.disa.mil/app/login/redirect/home**

3.4.2.3. The AFOCD includes current list of activity codes and SEIs as wel as is located on the myPers portal: **https://gum-crm.csd.disa.mil/app/login/redirect/home**

3.4.2.4. Do not replace existing SEIs.

Table 3.3. Military Personnel SEIs.

Certification Level	Enlisted SEIs	Officer SEIs
IAT Level I	260	C61
IAT Level II	264	C62
IAT Level III	265	C63
IAM Level I	266	C0I
IAM Level II	267	C0J
IAM Level III	268	C0K
CND-SP Analyst	872	See ***Note***
CND-SP Infrastructure Support	873	See ***Note***
CND-SP Incident Responder	874	See ***Note***
CND-SP Auditor	875	See ***Note***
CND-SP Manager	876	See ***Note***
IASAE Level I	See ***Note***	See ***Note***
IASAE Level II	See ***Note***	See ***Note***
IASAE Level III	See ***Note***	See ***Note***
***Note*:** SAF/CIO A6 is coordinating SEIs for these categories. Once established, SAF/CIO A6 will distribute to the PMOs/units.		

3.4.3. Contractors. Contractor cybersecurity requirements (e.g. cybersecurity certifications, clearances, computing environment/operating system training completion certificates, etc.) must be annotated in the PWS, new contract, or modified contract **(T-0)**.

3.4.3.1. Mandatory Contract Language. DoD has developed standard contract language for the cybersecurity WIP requirements section. Regarding cybersecurity workforce management requirements in contracts/PWS, the DoD CIO has coordinated with the Undersecretary of Defense for Acquisition, Technology, and Logistics (AT&L), Defense

Acquisition Regulations (DARs) Council to include language in DFARS. The coordinated DFARS section must be included as follows IAW **Figure 3.1(T-0)**.

Figure 3.1. DFARS Mandatory Contract Language.

252.239-7001 Information Assurance Contractor Training and Certification. As prescribed in 239.7103(b), use the following clause:

INFORMATION ASSURANCE CONTRACTOR TRAINING

AND

CERTIFICATION

(JAN 2008)

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

(End of clause)

3.4.3.2. For additional details, please see DoDD 8570.01 Information Assurance Training, Certification and Workforce Management Frequently Asked Questions at: **http://iase.disa.mil/iawip/Pages/iaetafaq.aspx**.

3.4.3.3. The PMO/unit should contact the procuring contracting office for guidance related to the FAR and its supplements. Contractor personnel will possess a DoD approved cybersecurity baseline certification(s) in good standing, commensurate with contract requirements by the first day of work **(T-0)**. The AF does not fund certification training, maintenance fees, or exam vouchers for contractors.

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 in identifying 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 to an UTC where the Mission Capability Statement (MISCAP) states 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/specialty and level IAW DoD 8570.01-M Table AP3.T1. SAF/CIO A6 will provide criteria and reporting instructions for each category/specialty and level. PMOs/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.

4.1.2. Possess a signed privileged access statement, if applicable.

4.1.3. Possess CND baseline certification, in good standing.

4.1.4. Possess appropriate and current personnel security investigation (e.g. NAC, SSBI, etc.) commensurate with assigned duties.

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

4.1.6. Complete an OJE, if applicable.

4.2. Computing Environment/Operating System Training Completion Certificate. IAW DoD 8570.01-M Table AP3.T1, All IATs and CND-SP (except for CND-SPM position) specialty personnel will complete training (e.g. formal, computer based training [CBT], web-based, or classroom instruction) on the operating system(s) and/or any security devices/services/tools the PMO/unit supports **(T-0)**. This requirement must apply to civilian, military, and contractor personnel who are required to attain/possess/maintain an IAT or CND-SP (except for CND-SPM position) cybersecurity baseline certification **(T-0)**. This training must provide the individual with a completion certificate **(T-0)**. The completion certificate(s) must be filed in the individual's training records **(T-3)**.

4.3. Privileged Access Agreement. IAW DoD 8570.01-M, Paragraph C2.1.4 and Table AP3.T1, all cybersecurity workforce personnel requiring privileged access will complete and sign a Privileged Access Agreement **(T-0)**.

4.3.1. All IATs (Level I, Level II, and Level III) and individuals in CND-SP Specialty (except for CND-SP Manager) positions will have a Privileged Access Agreement **(T-0)**.

4.3.2. The Agreement must explicitly state the position responsibilities **(T-0)**. The individual will sign the Privileged Access Agreement prior to gaining access to network or IS/PIT system **(T-0)**. Digital signatures are acceptable.

4.3.3. The WCO will maintain a copy of the signed Privileged Access Agreement **(T-3)**.

4.4. Additional CND Certification Requirement. Those individuals assigned to CND-SP positions will achieve the DoD approved CND certification as described in **Paragraph 3.2.7 (T-0)**.

Chapter 5

CYBERSECURITY WORKFORCE CERTIFICATION PROCESS

5.1. Cybersecurity Baseline Certifications.

5.1.1. Civilian, military, and contractor personnel assigned to a cybersecurity workforce position will possess and maintain in good standing a requisite DoD approved cybersecurity baseline certification(s) IAW DoD 8570.01-M, Paragraph C2.3.7 **(T-0)**. Contractors will be certified no later than the first day of contract work IAW DoD 8570.01-M, Paragraph C2.3.9 **(T-0)**.

5.1.2. Civilian and military personnel requiring certification will not be granted unsupervised privileged access until the appropriate certification or waiver, as described in **Chapter 8**, is attained IAW DoD 8570.01-M, Paragraph C3.2.4.6 **(T-0)**.

5.1.3. DoD does not recognize cybersecurity certifications that do not have a continuing education component.

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

5.2.1. The AF has a preferred list of DoD approved cybersecurity baseline certifications. The AF preferred list can be found at this link: **https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/A6SF/8570/default.aspx**. Those certifications on the AF preferred list have priority for funding.

5.2.2. Even though AF has a preferred list, personnel can attain/maintain certification from the DoD approved cybersecurity baseline certification list that is category/specialty and level specified for the assigned position.

5.3. Minimum Cybersecurity Baseline Certification Requirement for Five Enlisted AFSCs (3D0X2, 3D0X3, 3D1X1, 3D1X2, and 1B4X1). Certain military enlisted personnel have mandatory certification requirements. Personnel in the 3D0X2, 3D0X3, 3D1X2, and 1B4X1 AFSCs will attain and maintain, at a minimum, an IAT Level II cybersecurity baseline certification **(T-1)**. Personnel in the 3D1X1 AFSC will attain and maintain, at a minimum, an IAT Level I cybersecurity baseline certification, effective until 30 October 2015 **(T-1)**. Effective 31 October 2015, the 3D1X1 AFSC will transition to a new minimum certification, an IAT Level II cybersecurity baseline certification **(T-1)**. All 3D1X1 personnel will attain and maintain, at a minimum, an IAT Level II cybersecurity baseline certification by 31 October 2016 **(T-1)**. Personnel in these five career fields will maintain currency in a DoD approved certification applicable to category **(T-1)**. ***Note:*** A higher level certification may be required for assigned position.

5.3.1. Exam. AF centralized funds pay for one (1) exam voucher at the specified AFSC requirement unless member occupies an assigned position with different/higher cybersecurity requirements.

5.3.1.1. Through 30 October 2015, personnel in 3D1X1 AFSC can request one exam voucher for either an IAT Level I or IAT Level II cybersecurity baseline certification.

5.3.1.2. AF centralized funds 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/specialty, or multiple cybersecurity baseline certifications.

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

5.3.3. Military personnel in 3D0X2, 3D0X3, 3D1X1, 3D1X2, and 1B4X1 AFSCs will maintain the highest level baseline certification attained in good standing, to meet AFSC requirement, even while serving in a joint or special duty assignment **(T-1)**.

5.3.4. 3D CMSgts/SMSgts. Cybersecurity certifications are not mandatory for 3D CMSgts/SMSgts, except for those members assigned to cybersecurity-coded positions. The AF centralized funds will pay certification maintenance fees for those individuals already possessing a DoD-approved certification off the AF preferred list. The AF centralized funds will not provide exam vouchers for new certifications for CMSgts and SMSgts unless filling a cybersecurity-coded position.

5.4. Future Minimum Cybersecurity Baseline Certification Requirements for 17X Officer Career Field. To be prepared for the future and fast-paced challenges in cyberspace, 17Xs require a solid foundation in cybersecurity. Graduates of Undergraduate Cyber Training (UCT) will continue to attain IAM Level I cybersecurity baseline certification as a precondition for matriculation into the career field **(T-1)**. The intention is for the 17X Company Grade Officers (CGOs) (O-1 to O-3 ranks) to possess, at a minimum, an IAM Level I cybersecurity baseline. Going forward, 17X Field Grade Officers (FGOs) (O-4 to O-5 ranks) will attain and maintain, at a minimum, an IAM Level II cybersecurity baseline certification demonstrating increased foundational knowledge and continued professional progression **(T-1)**. Certifications for Colonels will be based upon assigned position requirements. The 17X career field manager is OPR for implementation guidance and policy.

5.4.1. If assigned to cybersecurity-coded position, 17X officers will attain required cybersecurity baseline certification within six (6) months of duty assignment **(T-1)**.

5.4.2. Exam Vouchers. Effective immediately, AF centralized funds will pay for one (1) Level I exam voucher from the AF preferred list for a CGO and one (1) IAM Level II exam voucher for 17X Captains, Majors and Lieutenant Colonels. Caveat: 17X officers, who use AF funds to attain IAM Level I certification as a Captain, must wait 18 months before they can request an IAM Level II exam voucher **(T-1)**. Otherwise, 17X Captains are encouraged to pursue their IAM Level II certification prior to promotion to the rank of Major. Attainment of IAM Level I is not a prerequisite to attain IAM Level II.

5.4.2.1. AF centralized funds will pay for additional exam voucher(s) from the AF preferred list when an individual is assigned to a cybersecurity coded position requiring a higher level certification requirement, certification in a new category/specialty, or multiple cybersecurity baseline certifications. An example is a 17X CGO is assigned to a cybersecurity-coded position, requiring an IAM Level III certification.

5.4.3. Maintenance. Individuals must comply with **Paragraph 5.8 (T-0)**.

5.4.4. Once cybersecurity baseline certification is attained, 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 AFSPC CYSS link: **https://cyss.us.af.mil/cyss/certifiedworkforce**.

5.5.1. Personnel assigned to a cybersecurity workforce position (Civilian and Military Only). The AF centralized funds will pay for one (1) cybersecurity baseline certification exam to meet the category and level of the cybersecurity-coded position or AFSC requirement. Those certifications on the AF preferred list have priority for funding. An individual can request an exam voucher for a higher level cybersecurity baseline certification within the same category/specialty.

5.5.1.1. Exception: The AF centralized funds pay for an additional exam voucher(s) when an individual is assigned to a cybersecurity-coded position requiring multiple cybersecurity baseline certifications **(T-1)**. Those certifications on the AF preferred list have priority for funding.

5.5.2. Retirement/Separation Restriction: The AF centralized funds will not be used to pay for an exam voucher for civilian and military personnel who are within one (1) year of confirmed retirement or separation date.

5.6. Certification Exam Failure/Decertification. This section applies to every military member who fails cybersecurity baseline certification exams or does not possess the required cybersecurity baseline within six months of assignment of duties. Likewise, this section applies to civilians who do not possess the required cybersecurity baseline within six months of assignment of duties. Furthermore, this section applies to civilians, military, and contractors who become decertified. Military and civilians may be subject to administrative action if they do not attain or maintain baseline certifications.

5.6.1. Except for re-testing conducted at schoolhouses, AF centralized funds will not pay for any re-testing required after an initial exam failure or decertification for civilians or military. SAF/CIO A6 may make exceptions on a case-by-case basis. The individual will be responsible for paying to re-test. The PMOs/units may fund with internal resources for a re-testing.

5.6.2. Civilian, military, and contractor personnel who fail to maintain certification(s) in good standing will not be allowed privileged access IAW DoD 8570.01-M, Paragraph C3.2.4.6 **(T-0)**.

5.6.3. Civilian Personnel. If a civilian has not attained 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 duties unless under the direct supervision of a cybersecurity certified individual **(T-1)**. The commander determines appropriate actions IAW civilian personnel policies if civilian does not attain requisite cybersecurity baseline certification(s) within six months of duty assignment.

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 duties (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 duties, once baseline certification is attained.

5.6.3.3. Embedded Duty. Those embedded duties (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 duties, once baseline certification is achieved.

5.6.4. Military Personnel. Military personnel who fail their initial cybersecurity baseline certification exam may be placed in remedial supervised training (e.g. CBTs, hands-on training, or instructor-led training). If a military member has not attained a DoD approved cybersecurity baseline certification commensurate to category and level of assigned position within six months of assignment, then the commanders of PMOs/units will reassign cybersecurity duties 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 Attainment. Where attainment of a cybersecurity baseline certification is a requirement for matriculation (i.e. entry) into an AFSC, commanders will begin AFSC disqualification actions IAW AFI 36-2101, Paragraph 4.1 after second test failure **(T-1)**. Otherwise, commanders of PMOs/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 and will not be assigned nor perform any cybersecurity duties in which they are not certified IAW DoD 8570.01-M, Paragraph C2.3.9 **(T-0)**. Timelines for contractor software developers/engineers/programmers to be certified are noted in **Paragraph 3.2.8**. Any issues concerning contract cybersecurity certification requirements should be addressed through the procuring contracting office.

5.6.6. Decertification: Decertification includes those individuals whose certifications are terminated or expired (e.g. failure to meet CEU standards, failure to pay maintenance fees, etc.). Decertification equates to an "exam failure". If decertification occurs for the following individuals, the commander of the PMO/unit:

5.6.6.1. Military. Has the discretion to retain the individual or pursue other appropriate administrative actions.

5.6.6.2. Civilian. Determines the appropriate action(s) IAW local civilian personnel policies if civilian has not maintained requisite cybersecurity baseline certification(s). If desired, has the discretion to allow up to six (6) months additional time for recertification. However, the commander of PMO/unit will reassign cybersecurity duties to another

individual who has the appropriate certification in good standing until recertification is achieved **(T-1).**

5.6.6.3. Contractor. Must immediately remove the individual from the position according to contract provisions and in coordination with the CO **(T-0)**.

5.7. Continuing Education Units (CEUs). DoD approved cybersecurity baseline certifications require CEUs to stay current. Commercial certification providers define the criteria for acceptable continuing education units. All certification holders (civilians, military, and contractors) will adhere to CEU policies set by their respective certification provider(s) IAW DoD 8570.01-M, Paragraph C3.2.3.7 **(T-0)**. Some commercial certification providers may allow CEUs for work experience that is documented and verified. Also, CBTs may count toward CEUs (please check with the commercial certification provider) and are available via various DoD resources such as the AF e-Learning program for civilians and military. Also, the IASE portal at: **https://www.dmdc.osd.mil/appj/dwc/index.jsp** has CBTs available.

5.8. Maintenance of Cybersecurity Baseline Certifications.

5.8.1. Civilian, military, and contractor personnel will maintain the highest-level cybersecurity baseline certification attained for category or specialty as required by position, AFSC, or PWS **(T-1)**.

5.8.2. For civilian and military personnel, AF centralized funds will pay maintenance fees for 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.

5.8.2.1. For civilian and military personnel, AF centralized funds will pay maintenance fees for the highest level certification on the AF preferred list necessary to meet category/specialty requirements of assigned position or AFSC.

5.8.2.2. AF centralized funds 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.

5.8.2.3. AF centralized funds will pay maintenance fees for multiple cybersecurity baseline certifications on the AF preferred list, if the civilian or military member is assigned to a cybersecurity workforce position requires multiple certifications.

5.8.3. Civilian, military, and contractor personnel will authorize a new certification release, whenever a certification is issued or renewed, to DoD/DMDC IAW DoD 8570.01-M, Paragraph C2.3.12 **(T-0)**. Personnel can access and submit release via DWCA on the DMDC portal: **https://www.dmdc.osd.mil/appj/dwc/index.jsp**.

5.8.4. Unless stipulated in contract(s), AF will not pay maintenance fees for contractors.

5.9. Recording Certification Completion. IAW DoD 8570.01-M, Paragraph C2.3.12, all personnel will authorize the certification provider to release the certification information status to DoD/DMDC.

5.9.1. Civilian. Civilian personnel can update civilian personnel database(s)/ 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 Air Force Personnel Services (AFPERS) application where it is verified by AFPC at Joint Base San Antonio (JBSA)-Randolph, TX. Once verified, the status in MyBiz would change to "Verified." Until the member uploads a copy of the certification in AFPERS, the member would remain in an uncertified status for reporting purposes.

5.9.2. Military. Military personnel (officers and enlisted) will complete AF Form 2096 to indicate award of the SEI for the highest cybersecurity certification attained, as indicated in the Enlisted or Officer Classification Directory **(T-1)**. 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, it is submitted to the appropriate servicing personnel function (FSS, MPF, or equivalent) for assignment to member's personnel record.

5.10. Recording Computing Environment/Operating System Training Completion. A computing environment/operating system training completion certificate must be awarded to meet computing environment/operating system training requirement IAW 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 Air Force, 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.

6.1.1. Cyberspace Defense Operations enlisted personnel (1B4), various Cyberspace Support enlisted personnel (3D), and Cyberspace Operations officers (17X) are provided initial cybersecurity certification training at schoolhouses, as listed below.

6.1.1.1. 3D1X1: Client Systems – IAT Level I – A+ CE .

Note: Valid only through 30 October 2015. Effective 31 October 2015, IAT Level II certification becomes the new initial skills training certification requirement. By 31 October 2016, 3D1X1 personnel will obtain a Security+ CE certification from successful completion of the initial skills training.

6.1.1.2. 3D0X2: Cyber Systems – IAT Level II – Security+ CE

6.1.1.3. 3D0X3: Cyber Surety – IAT Level I – Security+ CE

6.1.1.4. 3D1X2: Cyber Transport – IAT Level II – Security+ CE

6.1.1.5. 1B4X1: Cyberspace Defense Operations – IAT Level II – Security + CE

6.1.1.6. 17X: Cyberspace Operations Officers – IAM Level I – Security + CE

6.1.2. Enlisted and officers completing the Intermediate Network Warfare Training (INWT) course will receive a Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC) **(T-1)**.

6.1.3. Civilians and military personnel not in an AFSC listed in **Paragraph 6.1.1** can obtain training via distributive/online learning or unit-funded training courses.

6.2. Distributive/Online Learning. For those civilians or military personnel not in initial skill training program at an AF schoolhouse, distributive learning resources are available at no cost to civilian and military users via E-Learning on the AF Portal. Training material is also available on the AF Portal. AF Portal distributive learning resources are only accessible to government employees.

6.3. Authorizing Official (AO) Training. The AO will attain training through the DAA CBT located on the IASE portal: **http://iase.disa.mil/eta/Pages/index.aspx (T-0)**.

6.4. Contracted Training. PMOs/units may acquire, with their own funds, instructor-led training and virtual instructor-led training to provide certification specific training for personnel unable to attain certification through distributive learning.

6.5. Military Computing Environment/Operating System Training Options.

6.5.1. AF Specialty training schoolhouses/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/Operating System training not covered by formal AF Specialty

training, schoolhouse technical schools, or commercially available courses. The training can be accomplished through AF e-learning and IASE portal.

6.5.3. Computing Environment/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/unit.

6.6. Civilian Computing Environment/Operating System Training Options.

6.6.1. Use of CBTs or DoD developed classroom training is the preferred method for obtaining Computing Environment/Operating System training completion certificates. Training can be obtained through various sources like AF e-learning and the IASE portal.

6.6.2. Computing Environment/Operating System training completion certificates may be obtained from commercial sources. However, this training is at the discretion of and funded by the MAJCOM or individual PMO/unit.

6.7. Contractor Computing Environment/Operating System Training Options.

6.7.1. Contractor will be responsible for their own Computing Environment/Operating System training, unless otherwise stated in the PWS **(T-3)**.

Chapter 7

CYBERSECURITY WORKFORCE REPORTING METRICS AND VALIDATION

7.1. Reporting. The AF cybersecurity workforce will be managed and reported through the use of manpower and personnel database(s)/system(s) **(T-0)**. However, contractor data is tracked locally, usually by the CO designated technical representative(s).

7.2. Metrics. PMOs/units must report the status of their cybersecurity workforce (civilian, military, and contractors) qualifications **(T-1)**. SAF/CIO A6 will provide the instructions on reporting requirements, including the criteria, template, and reporting frequency. A sample metric format is provided in **Attachment 4**. At present, AF does not have a centralized/consolidated database or system to track contractor cybersecurity requirements. Therefore, contractor requirements must be tracked locally **(T-1)**.

7.3. Annual Cybersecurity Position Validation: Annually, the PMOs/units must conduct, review, and validate every cybersecurity workforce position (civilian and military) on the UMD and the data in personnel databases/systems such as DCPDS for civilians and MILPDS for military **(T-1)**. The SAF/CIO A6 will provide instructions on reporting requirements such as template and suspense dates.

Chapter 8

CYBERSECURITY BASELINE CERTIFICATION WAIVERS (CIVILIANS AND MILTARY ONLY)

8.1. IAW 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 AO has the authority to suspend temporarily via waivers the 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 IS/PIT system under the AO's responsibility. The waivers must not be authorized for contractor personnel IAW DoD 8570.01-M, Paragraphs C3.2.4.1.1, C4.2.3.2, and C11.2.4.1.1 **(T-0)**.

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

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

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

8.2.3. The waiver must state an expiration date and must not exceed more than 6 months except for deployment exception listed in **Paragraph 8.2.5 (T-0)**. Consecutive waivers are not authorized.

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

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

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

8.2.7. The PMO/unit must provide a copy of the AO-signed waivers to the AF SISO **(T-1)**.

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

WILLIAM J. BENDER, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5, U.S.C., Section 552a, as amended, *The Privacy Act of 1974*

National Defense Authorization Act for Fiscal Year 2013

Committee on National Security Systems 4016, *National Information Assurance Training Standard For Risk Analysts*, 1 November 2005

DoD 5200.2-R, *Personnel Security Program Including Administrative Change 3 dated 23 February 1996)*, January 1987

DoD Directive 8570.01, *Information Assurance (IA) Training, Certification and Workforce Management*, 15 August 2004

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

DoD Instruction (DoDI) 1336.05, *Automated Extract of Active Duty Military Personnel Records*, 28 July 2009

DoDI 7730.64, *Automated Extracts of Manpower and Unit Organizational Element Files*, 11 December 2004

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DODI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014

DoD 8570.01-M, *Information Assurance Workforce Improvement Program, Change 3*, 24 January 2012

Air Force Instruction (AFI) 33-200, *Information Assurance (/IA) Management*, 23 December 2008

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program*, 23 December 2008

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFI 36-2101, Classifying Military Personnel (Officer and Enlisted), 14 June 2010

AFI 36-701, *Labor Management Relations*, 27 July 1994

AFI 38-204, *Programming USAF Manpower*, 1 August 1999

Air Force Manual (AFMAN) 33-363, *Management of Records*, 1 March 2008

AFMAN 33- 282, *Computer Security* (COMPUSEC), 27 March 2012

International Organization for Standardization/International Electro-technical Commission ISO/IEC 17024, *Conformity Assessment – General Requirements for Bodies Operating Certification of Persons*, 1 April 2003

Adopted Forms

DD Form 2875, System Authorization Access Request (SAAR), August 2009

AF Form 847, Recommendation for Change of Publication, 22 September 2009

AF Form 2096, Classification/On-the-Job Training Action, 26 March 2014

Abbreviations and Acronyms

AF—Air Force

AFPERS—Air Force Personnel Services

ANG—Air National Guard

AFRC—Air Force Reserve Command

AO—Authorizing Official

BI—Background Investigation

CBT—Computer Based Training

CEU—Continuing Education Unit

CFM—Career Field Manager

CIA—Confidentiality, Integrity, and Availability

CIO—Chief Information Officer

CND—Computer Network Defense

CND-A—Computer Network Defense Analyst

CND-AU—Computer Network Defense Auditor

CND-IR—Computer Network Defense Incident Responder

CND-IS—Computer Network Defense Infrastructure Support

CND-SP—Computer Network Defense Service Provider

CND-SPM—Computer Network Defense Service Provider Manager

CO—Contracting Officer

CPCN—Civilian Position Control Number

CPD—Core Personnel Document

COCOM—Combatant Command

CSSLP—Certified Secure Software Lifecycle Professional

DAA—Designated Accrediting Authority

DCPDS—Defense Civilian Personnel Data System

DEERS—Defense Eligibility Enrollment Reporting System

DISA—Defense Information Systems Agency

DMDC—Defense Manpower Data Center

DoD—Department of Defense

DoD CIO—DoD Chief Information Officer

DoDIN—DOD Information Network

DoD SAPCO—DoD Director, Special Access Programs Central Office

DRU—Direct Reporting Units

FISMA—Federal Information Security Management Act

FN—Foreign National

FOA—Field Operating Agency

GIAC—Global Information Assurance Certification

GSEC—GIAC Security Essentials Certification

HBSS—Host Base Security System

IA—Information Assurance

IAM—Information Assurance Management Category

IAO—Information Assurance Officer

IASE—Information Assurance Support Environment

IASAE—Information Assurance System Architect and Engineer

IAT—Information Assurance Technical

IAW—In Accordance With

IC—Intelligence Community

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

INWT—Intermediate Network Warfare Training

IS—Information System

ISC2—International Information Systems Security Certification Consortium

ISO/IEC—International Organization for Standardization/International Electro-technical Commission

ISSO—Information System Security Officer

ISSM—Information System Security Manager

IT—Information Technology

LN—Local National

MAJCOM—Major Command

MILPDS—Military Personnel Data System

MPCN—Manpower Position Control Number

MPES—Manpower Programming and Execution System

NE—Network Environment

ODNI—Office of Director of National Intelligence

OE—Operating Environment

OJE—On-the-Job Evaluation

OPM—Office of Personnel Management

OS—Operating System

OSD—Office of the Secretary of Defense

PD—Position Description

POM—Program Objective Memorandum

PWS—Performance-Based Work Statement

SA—System Administrator

SAP—Special Access Program

SISO—Senior Information Security Officer

SEI—Special Experience Identifier

SP—Service Provider

SRG—Security Recommendation Guide

SSBI—Single Scope Background Investigation

STIG—Security Technical Implementation Guide

UCT—Undergraduate Cyberspace Training

UMD—Unit Manning Document

UTM—Unit Training Manager

WCO—Wing Cybersecurity Office

WIP—Workforce Improvement Program

Attachment 2

AF CYBERSECURITY POSITION CERTIFICATION DETERMINATION GUIDE

Table A2.1. Technical Category.

Duties	IAT Level I	IAT Level II	IAT Level III	Other
Conduct general system management - standalone (non-networked) server/workstation/ end user device only - create /modify e-mail group mailbox; create/delete e-mail account; create/modify user account; download/install standard functional drivers and operating system; install peripherals (printers, scanners, etc.); lock/unlock user account; modify account privilege(s); reset user password; run queries; view account properties; and/or view queries	X			
Create administrator account – standalone (non-networked) server/ workstation/end user device only	X			
Create/modify login scripts - standalone server workstation/end user device only	X			
Download/install security drivers – standalone (non-networked) server workstation/end user device only	X			
Has root level network access - standalone (non-networked) server/workstation/ end user device only	X			
Install/update security software, including definitions, on standalone (non-networked) server/ workstation/end user device only	X			
Lock/unlock administrator account – standalone (non-networked) server/workstation/ end user device only	X			
Perform system backups - standalone (non-networked) server/workstation/ end user device only	X			
Reset administrator account password - workstation/end user device only	X			
Conduct general system management - networked, but on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems: create /modify e-mail group mailbox; create/delete e-mail account; create/modify user account; download/install		X		

Duties	IAT Level I	IAT Level II	IAT Level III	Other
standard functional drivers and operating system; install peripherals (printers, scanners, etc.); lock/unlock user account; modify account privilege(s); reset user password; run queries; view account properties; and/or view queries				
Create administrator account(s) on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Create/modify login scripts on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Download/install security drivers on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Has access rights to networked security devices and/or tools such as routers, firewalls, intrusion detection/prevention systems, host based security system (HBSS) supporting interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Has root level network access on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Install/update security software, including definitions, on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Lock/unlock administrator account on interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Perform system backups on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be		X		

Duties	IAT Level I	IAT Level II	IAT Level III	Other
localized only to networked systems				
Push security software/updates on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts can be localized only to networked systems		X		
Reset administrator account password on interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Conduct general system management - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s): create /modify e-mail group mailbox; create/delete e-mail account; create/modify user account; download/install standard functional drivers and operating system; install peripherals (printers, scanners, etc.); lock/unlock user accounts; modify account privileges; reset user passwords; run queries; view account properties; and/or view queries			X	
Conduct technical audits/validations of security controls for enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Create administrator account - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible server			X	
Create/modify login scripts - enterprise (i.e. has potential global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Download/install security drivers – enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Has access rights to networked security devices and/or tools such as routers, firewalls, intrusion detection/prevention systems, Host Based Security System (HBSS) - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	

Duties	IAT Level I	IAT Level II	IAT Level III	Other
Has root level network access - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Install/update security software - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Lock/unlock administrator account - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Perform system backups - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Push security software/ updates – enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Reset administrator account password - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Update antivirus definitions - enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Performs software design, code development/writing, code compiling, software testing, etc., support IS(s)/PIT system(s) - less than 4 years of experience				Please refer to **Para 3.2.12**.
Performs software design, code development/writing, code compiling, software testing, etc., support IS(s)/PIT system(s) - more than 4 years of experience				Please refer to **Para 3.2.12.**

Table A2.2. Management Category.

Duties	IAM Level I	IAM Level II	IAM Level III	Other
Assist in the development of cybersecurity assessment and authorization documentation	X			

Duties	IAM Level I	IAM Level II	IAM Level III	Other
Collect and maintain data needed to meet server cybersecurity reporting requirements	X			
Develop/modify cybersecurity program plans and requirements for standalone (non-networked) server only	X			
Develop procedures to ensure system users are aware of their cybersecurity responsibilities before granting access to IS(s)/PIT system(s)	X			
Ensure system security configuration guidelines are followed	X			
Ensure cybersecurity requirements are appropriately identified in standalone (non-networked) server only procedure	X			
Monitor system performance and review for compliance with security and privacy requirements on standalone (non-networked) server only	X			
Recognize a possible security violation and take appropriate action to report the incident, as required	X			
Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered	X			
Support and administer data retention and recovery on standalone (non-networked) server only	X			
Use federal and organization specific published documents to manage operations on standalone (non-networked) server only	X			
Advise the Authorizing Official (AO) of any changes affecting the interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Assist in the gathering and preservation of evidence used in the prosecution of computer crimes		X		

Duties	IAM Level I	IAM Level II	IAM Level III	Other
Conduct physical security assessment and correct physical security weaknesses on an interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Develop cybersecurity requirements, specific to interconnected/ networked IS(s))/ PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems acquisition for inclusion in procurement documents		X		
Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for the interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow cybersecurity policies and procedures for interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Ensure that compliance monitoring occurs, and review results of such monitoring across the interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Ensure that cybersecurity inspections, tests, and reviews are coordinated for the interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Ensure that cybersecurity and cybersecurity-enabled software, hardware, and firmware comply with appropriate security configuration guidelines, policies, and procedures for interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Ensure recovery processes are monitored and that cybersecurity features and procedures are properly restored for interconnected/networked		X		

Duties	IAM Level I	IAM Level II	IAM Level III	Other
IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems				
Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Evaluate and validate security controls in support of assessment and authorization (formerly called certification and accreditation) activities for final determination by the AO		X		
Identify alternative cybersecurity strategies to address interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Monitor contract performance and periodically review deliverables for conformance with contract requirements related to cybersecurity and privacy for interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Oversee the preparation of cybersecurity assessment and authorization documentation for interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Provide leadership and direction to personnel supporting interconnected/networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems by ensuring that cybersecurity security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities		X		

Duties	IAM Level I	IAM Level II	IAM Level III	Other
Recommend resource allocations required to securely operate and maintain interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems cybersecurity requirements		X		
Review cybersecurity security plans for the interconnected/ networked IS(s)/PIT system(s) where systems are not accessible AF-wide and impacts are localized only to networked systems		X		
Review the selected security safeguards to determine that security concerns identified in the approved plan have been fully addressed		X		
Support cyber security assessment of security controls and conduct initial remediation actions in preparation for system authorization using DoD assessment procedures such as Security Recommendation Guides (SRG) & Security Technical Implementation Guides (STIGs)		X		
Advise the Authorizing Official (AO) of changes affecting the enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s) cybersecurity posture.			X	
Approve cybersecurity assessment and authorization documentation			X	
Analyze, develop, approve, and issue cybersecurity policies for enterprise (i.e. have potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s) cybersecurity policies			X	
Analyze identified security strategies and select the best approach or practice for the enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Ensure information ownership responsibilities are established for each enterprise (i.e. have potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s)			X	
Ensure that protection and detection capabilities are acquired or developed for enterprise (i.e. have			X	

Duties	IAM Level I	IAM Level II	IAM Level III	Other
potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s)				
Ensure that security related provisions of the system acquisition documents meet all identified security needs for enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s) /PIT system(s)			X	
Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed for enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Evaluate cost benefit, economic and risk analysis in decision making process enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Evaluate proposals to determine if proposed security solutions effectively address enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s) requirements, as detailed in solicitation documents			X	
Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents for enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Identify IT security program implications of new technologies or technology upgrades			X	
Interpret and/or approve cybersecurity requirements relative to the capabilities of new information technologies			X	
Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise (i.e. have potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s) cybersecurity program			X	

Duties	IAM Level I	IAM Level II	IAM Level III	Other
Monitor and evaluate the effectiveness of the enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s) cybersecurity security procedures and safeguards to ensure they provide the intended level of protection			X	
Oversee the preparation of cybersecurity assessment and authorization documentation for enterprise (i.e. have potentially global impacts to AF missions/operations/ business activities/users) accessible IS(s)/PIT system(s)			X	
Provide enterprise (i.e. have potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s) cybersecurity guidance for development of the Continuity of Operations Plan (COOP)			X	
Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enterprise (i.e. have potentially global impacts to AF missions/operations/business activities/users) accessible IS(s)/PIT system(s)			X	
Take action as needed to ensure that accepted products meet Common Criteria requirements			X	

Attachment 3

MILITARY CERTIFICATION FAILURE POLICY (INITIAL CERTIFICATION ATTAINMENT)

Table A3.1. Failure Policy Matrix.

Individuals who've	**Resulting in**	**Result(s)**	**Responsible Authority**	**Actions(s) Taken**
Completed **first** cybersecurity certification exam attempt	Passing score	Individual cleared to perform cybersecurity duties	Supervisor	Assign individual as appropriate
	Failing score	Individual can be placed in remedial, supervised training (CBTs, Advanced Distributed Learning Service (ADLS), hands- on training, etc.)	Commander and Supervisor	The commander of PMO/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 duties, the commander (PMO/unit) will reassign cybersecurity duties to another individual who has the appropriate certification in good standing until certification is achieved **(T-1).** 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 duties unless under the direct supervision of a cybersecurity certified individual **(T-1)**. Due to operational constraints, supervisor/commander could pursue a temporary AO approved waiver IAW **Chapter 8**.
Completed a **second** cybersecurity certification exam attempt	Passing score	Individual is cleared to perform cybersecurity duties	Supervisor	Assign individual as appropriate
	Failing score	Individual will not perform any cybersecurity duties, unless under the direct supervision of a cybersecurity certified individual **(T-1)**.	Commander and Supervisor	Where attainment of a cybersecurity baseline certification is a requirement for matriculation (i.e. entry) into an AFSC, commanders will begin AFSC disqualification actions IAW AFI 36-2101, Paragraph 4.1 after second test failure **(T-1)**. Otherwise, the commander (PMO/unit) has the discretion to retain the individual or pursue other appropriate administrative actions(s). The commander (PMO/unit) will reassign cybersecurity duties to

				another individual who has the appropriate certification in good standing until certification is achieved **(T-1).**

Attachment 4

SAMPLE CYBERSECURITY WORKFORCE METRICS

1. Positions: By category/specialty (IAT, IAM, IASAE, and CND-SP) and level (Level I, II, and III), report the number of authorized cybersecurity positions.

a. Civilian

b. Military

2. Filled: By category/specialty (IAT, IAM, IASAE, and CND-SP) and level (Level I, II, and III), report the number of authorized cybersecurity positions.

a. Civilian

b. Military

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

a. Civilian

b. Military

c. Contractor

4. Computing Environment/Operating System Training Completion Certificates: This applies mostly to the IAT category and Computer Network Defense –Service Provider (CND-SP) Specialty (except for CND-SP Manager). By category/specialty (IAT and CND-SP) and level (Level I, II, and III), report the number of cybersecurity personnel with privileged access and documented proof of completing training on the software and/or security tool(s)/devices that individual supports in performance of cybersecurity duties.

a. Civilian

b. Military

c. Contractor

6. OJE. This applies only to the IAT category and CND-SP Specialty (except for CND-SP Manager). By category/specialty (IAT and CND-SP) 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

7. Signed Privileged Access Statement: This applies to the IAT category, select IAM with privilege access, and CND-SP Specialty (except for CND-SP Manager). By category/specialty (IAT, IAM, and CND-SP) and level (Level I, II, and III), report the number with signed agreements by the individual and supervisor/management, outlining access responsibilities.

a. Civilian

b. Military

c. Contractor

8. Personnel Security Investigation: By category/specialty (IAT, IAM, IASAE, and CND-SP) 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

9. Qualified: By category/specialty (IAT, IAM, IASAE, and CND-SP) and level (Level I, II, and III), report the number who have completed all of the requirements for their respective category and level IAW **Chapter 4** and of DoD 8570.01-M, Table AP3.T1.

a. Civilian

b. Military

c. Contractor

10. Waivers: Report the number of cybersecurity personnel who have approved waivers.

a. Civilian

b. Military

11. 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

Attachment 5

SAMPLE - FORMAL STATEMENT OF RESPONSIBILITIES

(Applicable for Civilians and Military)

CYBERSECURITY-CODED POSITION (UMD):_____
1. I understand that I am assigned to the above position and expected to perform the following cybersecurity functions:

1. Cybersecurity Functions 1:

2. Cybersecurity Functions 2:

N. Cybersecurity Function N:

(Paragraph 1: To Be Completed By Supervisor)

2. I understand I will attain and maintain the appropriate DoD approved cybersecurity baseline certification(s) applicable for the cybersecurity functions assigned above and required for the above position IAW DoD 8570.01-M.

Individual's Name _____
Individual's Signature_____
Date_____
Supervisor's Name _____
Supervisor's Signature _____
Date_____

KEEP SIGNED DOCUMENT LOCALLY

Attachment 6

SAMPLE - FORMAL STATEMENT OF RESPONSIBILITIES

(Applicable for Contractors)

CYBERSECURITY POSITION (CONTRACTUAL TITLE)_____
1. I understand that I am assigned to the above position and expected to perform the following cybersecurity functions:

1. Cybersecurity Function 1:

2. Cybersecurity Function 2:

N. Cybersecurity Function N:

(Paragraph 1: To Completed By Contracting Officer (CO)/CO Designated Technical Representative)

2. I understand I will attain and maintain the appropriate DoD approved cybersecurity baseline certification(s) applicable for the cybersecurity functions assigned above and required for the above position IAW DoD 8570.01-M

Individual's Name_____
Individual's Signature _____
Date_____
CO Designated Technical Representative's Name_____
CO Designated Technical Representative's Name _____
Date_____

KEEP SIGNED DOCUMENT LOCALLY