DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

Personnel Security Investigation Requirements And Training Requirements

Blue font is for informational purposes.

Black font includes example language for the government's requirements.

1.0 Personnel Security Investigation Requirements

The types of Personal Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon government requirements and the work the contractor will perform.

Contractors shall provide a listing of personnel who require a Common Access Card (CAC) to the Contracting Office (CO) and Trusted Associate. The contractor shall submit on company letterhead the names, Cybersecurity position(s) the employee will fill, the date and appropriate certification for the Cybersecurity position, CDRL _____, Contractor's Personnel Roster. Reference paragraph 1.2 Additional PSI Requirements for Cybersecurity Workforce Positions for additional required information. The government Trusted Associate will verify each individual's clearance prior to sponsoring the individual for a CAC.

{Effective 1 March 2020[1], 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. The AFMAN has additional requirements for the remaining cybersecurity workforce roles.

Mandatory contract language. DoD has developed standard contract language for the cybersecurity Workforce Improvement Program requirements section. Regarding cybersecurity workforce management requirements in contracts/PWS, the DoD Chief Information Officer (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

[1] AFMAN17-1303_AFGM2016-01, *Air Force Guidance Memorandum to AFMAN33-285 CYBERSECURITY WORKFORCE IMPROVEMENT PROGRAM*, paragraph 3.2.12.2.

DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

follows in accordance with (IAW) DFARs 252.239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION.}

1.1 For All CAC-Eligible Individuals

A background investigation is required for contractors eligible for a CAC. Contractor personnel requiring a CAC must have a favorably adjudicated background investigation as stipulated in Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013, *http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf*.

1.2 Additional PSI Requirements for Cybersecurity Workforce Positions

AFMAN17-1303, AF CYBERSECURITY POSITION CERTIFICATION DETERMINATION GUIDE 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. 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. Individuals may access ADLS through this link: https://golearn.csd.disa.mil/kc/rso/login/ADLS_login.asp. As a secondary method, individuals may access this training on the Defense Information Systems Agency (DISA) DoD Cyber Exchange NIPR portal: https://cyber.mil/training/dod-authorizing-official-ao/. 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.,

DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

certification, training, etc.) specified in this manual are the minimum required. Commanders may increase requirements to reflect specific duties and or function(s).

This manual applies to Contractors (private sector employees - US citizens and Foreign Nationals) who are network users as well as those who are performing contractual cybersecurity support to the Air Force. Attachment 6 includes a sample formal statement of responsibilities.

In accordance with AFMAN17-1303, *AF CYBERSECURITY POSITION CERTIFICATION DETERMINATION GUIDE*, the contractor shall:

a. Attain appropriate cybersecurity certification(s) applicable for assigned cybersecurity workforce position ***prior to the first day of work on this task order*** IAW DoD 8570.01-M, Paragraph C2.3.9.
b. Maintain in good-standing cybersecurity baseline certification(s) IAW DoD 8570.01-M, Paragraph C2.3.7.
c. Maintain the highest-level cybersecurity baseline certification attained for category or specialty as required by position within this PWS.
d. Become qualified in cybersecurity position as defined in AFMAN 17-1303 Chapter 4 WORKFORCE QUALIFICATIONS.
e. 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.
f. 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. ***An example agreement can be found in DoD 8570.01-M, Appendix 4.***
g. Authorize the release of cybersecurity baseline certification or a new certification release, whenever a certification is issued or renewed, to DoD/DMDC IAW DoD 8570.01-M, Paragraphs C2.3.12. The authorization release can be found: https://dmdc.osd.mil/appj/dwc/index.jsp.
h. Not be reimbursed for certification costs or maintenance fees.
i. Not be eligible for cybersecurity baseline certification waivers IAW DoD 8570.01-M, Paragraphs C2.3.9.
j. Report their workforce certifications on CDRL _____, Contractor's Personnel Roster.

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.

DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

Work performed on this task order is required to fill the following Cybersecurity Workforce positions: ***{Refer to AFMAN 17-1303, Chapter 5 CYBERSECURITY WORKFORCE CERTIFICATION PROCESS.}***

{List the positions with a brief description. Example.}

1.2.1 Information Assurance Technical (IAT)-II

{Use the wording from the AFMAN17-1303 for the position description from Chapter 3 CYBERSECURITY.}

1.2.2 IA System Architect and Engineer (IASAE)-I

{Use the wording from the AFMAN17-1303 for the position description.}

1.2.3 Computer Network Defense – Service Provider (CND-SP)[2]

{Use the wording from the AFMAN17-1303 for the position description such as: CND-SP Analyst (CND-A), CND-SP Infrastructure Support (CND-IS) or CND-SP Incident Responder (CND-IR).}

1.2.4 Confirming compliance with Cybersecurity Workforce Requirements

The contractor shall provide the following additional information to the CO for each individual filling a Cybersecurity Workforce position:

a. Proof the individual possess a DoD-approved cybersecurity baseline certification, in good standing

   1. Individuals shall possess a DoD-approved cybersecurity baseline certification commensurate to category and level of the assigned position. The public version of the DoD Cyber Exchange provides a summary of IA workforce qualification requirements: https://public.cyber.mil/cwmp/summary/.

   2. 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

[2] The mandated change in AFI17-1303 (effective March 2020) does not apply to the Computer Network Defense-Service Provider Manager position, reference paragraph 4.2 in the AFI.

DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

b. A signed privileged access statement, if applicable. 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[3].

c. Confirmation the individual possess appropriate and current personnel security investigation (e.g. Tier 3) commensurate with assigned duties.

d. Proof the individual possess computing environment/operating system training completion certificate(s) on all operating systems and/or security-related tool(s)/devices supported by the ***{system name},*** as applicable to the Cybersecurity Workforce position[4]. ***{Identify the computing environment/operating system training requirement.}***

1.3 Annual Requirement for Cyber Awareness and Force Protection Training

All contractor personnel shall complete the Information Protection, *DoD Information Assurance Awareness (IAA) Cyber Awareness Challenge and Force Protection* computer base training and other security related training as directed prior to the government granting access to an IS. Contractor personnel shall accomplish the Cyber Awareness and Force Protection training annually using the Advanced Distance Learning System (ADLS) computer-based 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) DoD Cyber Exchange NIPR portal: https://cyber.mil/training/dod-authorizing-official-ao/.

2.0 Services Delivery Summary

CPAR Area[5]	PWS Para	Performance Threshold	Assessment
Quality Software Engineering	1.2 and 1.3	Prior to starting work on the task order, contractor personnel possess all DoD and AF certifications as identified. The Contractor maintains the required certifications as appropriate for the positions filled.	Assess the contractor's success with respect to: Staffing with the software knowledge, skills, and abilities needed to execute the task order across the lifecycle; timely assignment of the appropriate numbers of software staff

[3] DoD 8570-01-M, Appendix 4, SAMPLE STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf
[4] AFMAN17-1303_AFGM2016-01, paragraph 4.1, Qualified Cybersecurity Workforce Criteria
[5] CPARS Guidance, Evaluation Areas

DISCLAIMER: This document is provided to assist users in defining their requirements. The user is responsible for verifying the latest DoD or AF standards are identified in their task orders and for knowing and documenting their requirement(s).

CPAR Area[5]	PWS Para	Performance Threshold	Assessment
Management Program management and other management	1.2 and 1.3	Prior to starting work on the task order, contractor personnel possess all certifications and meet DoD and AF certifications as identified. The Contractor maintains the required certifications as appropriate for the positions filled.	Assess the extent to which the contractor discharges its responsibility for integration and coordination of all activity needed to execute the contract/order; ***identifies and applies resources required to meet schedule requirements; assigns responsibility for tasks/actions required by the task order***; communicates appropriate information to affected program elements in a timely manner.

3.0 Resources

3.1 DoD 5010.12-M Procedures for the Acquisition and Management of Technical Data

The purpose of this manual is to provide a uniform approach to the acquisition and management of data required from contractors. The procedures are intended to provide data management tools necessary to minimize and standardize data requirements that will be included in DoD contracts.

This manual provides step-by-step instructions for completing the DD Form 1423 in Chapter 3, Acquisition of Data.

Source:
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501012m.pdf?ver=2018-12-20-144750-287

3.2 Contract Data Requirements List (CDRL), DD Form 1423

The standard format for identifying potential data requirements in a solicitation and deliverable data requirements in a contract.

Where to download the DD Form 1423:
https://www.esd.whs.mil/Directives/forms/dd1000_1499/

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY: TDP _____ TM _____ OTHER X - ADMN

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
	CONTRACTOR'S PERSONNEL ROSTER		

4. AUTHORITY *(Data Acquisition Document No.)*	5. CONTRACT REFERENCE	6. REQUIRING OFFICE	18. ESTIMATED TOTAL PRICE
DI-MGMT-81834A			

7. DD 250 REQ	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
LT	D	ONE/R	10DAC

8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION
See Blk 16	See Blk 16	R/ASREQ

16. REMARKS

Block 4: Contractor shall use DI-MGMT-81834A as the submittal template, removing item 2.1.s and adding: the Cybersecurity Workforce position(s) filled (use N/A) if not applicable; the DoD-approved cybersecurity baseline and date of certification; the type of personal security investigation and date; computing environment/operating system training and date; date of Cyber Awareness and Force Protection training.

Block 8: Submissions shall not include macros, passwords, program executables, embedded objects or external links. The Government has (10) business days to review for correct content and format. If correction is warranted, the contractor has (5) business days after notice to correct deficiencies and re-submit. Criteria for approval shall be correct content and format (if applicable).

Block 10: One time with revisions.

Block 11: As of the date of the CDRL title/signature page.

Block 12: 10 calendar days after contract start date.

Block 13: Revisions as data within the CDRL changes. Updates required by the 6th day of the next month when employee information changes.

Block 14: The Government requires all deliverables that include Personal Identifiable Information (PII) be properly marked and encrypted. However, email should be the last medium used to deliver PII. DoD SAFE is the preferred method of delivery and can be accessed through the following website: https://safe.apps.mil/

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
See Blk 16			
15. TOTAL →	0	0	0

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE

Reset