



Communications and Information

INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

---

**NOTICE:** This publication is available electronically on the USTRANSCOM electronic library.

**RELEASABILITY:** There are no releasability restrictions on this publication

---

OPR: TCJ6-OIP

Approved By: TCJ6 (Brig Gen Earl D. Matthews)

Pages: 9

Distribution: e-Publishing

---

This instruction provides the policies and procedures for implementing Department of Defense Manual (DODM) 8570.01-M, *Information Assurance Workforce Improvement Program*. It is applicable to all United States Transportation Command (USTRANSCOM) personnel performing information assurance duties delineated in DOD 8570.01-M. Failure to comply with the provisions of this instruction may result in removal from or inability to serve in an Information Assurance Workforce Improvement Program (IAWIP) designated position. Refer recommended changes and questions about this instruction to the Office of Primary Responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this instruction are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

**1. References and Supporting Information.** References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

**2. Overview.**

**2.1.** All personnel (military, civilian, and contractor) assigned to perform Information Assurance (IA) functions and in an identified IAWIP position as delineated in DODM 8570.01-M must be appropriately certified. Personnel must be certified even if the IA functions assigned are an additional duty.

**2.2.** IAWIP positions must be identified in appropriate manpower systems and explicitly identified in contracts. Positions must be identified by both category (Information Assurance Technical (IAT), Information Assurance Management, Information Assurance System Architect and Engineer, and Computer Network Defense Service Provider) and level (I, II and III), as defined in DODM 8570.01-M. For IATs with privileged access, computing environment certification requirements must also be identified and an on the job evaluation accomplished.

**2.3.** Sustainment costs of USTRANSCOM's IAWIP program will be covered through normal Service funding channels for military and civilian personnel. IAWIP requirements for contractor personnel will be included in Performance Work Statements (PWS).

### **3. Roles and Responsibilities.**

**3.1.** IAWIP Program Manager will:

**3.1.1.** Maintain this instruction in accordance with USTRANSCOM Instruction 33-24, *Publications and Forms Management*.

**3.1.2.** Maintain and provide IAWIP statistics to USTRANSCOM Command, Control, Communications and Computer Systems Directorate (TCJ6) Chief Information Office (CIO) and Distribution Portfolio Management Division (TCJ6-I) to support Federal Information Security Management Act (FISMA), and DOD compliance reporting.

**3.1.3.** Coordinate quarterly Certification Requirement Assessments to identify new IA positions.

**3.1.4.** Assist in identifying and acquiring computing environment certification training, such as computer based training (CBT) and Defense Information Systems Agency (DISA)-provided classes.

**3.1.5.** Provide information on continuing education opportunities, no-cost classes, etc., to support the staff in maintaining their certifications.

**3.1.6.** Assist supervisors with identification of remedial supervised training opportunities (CBTs, Advanced Distribution Learning Services, and hands-on training), as needed.

**3.2.** IAWIP Functional Program Manager will:

**3.2.1.** Provide overall functional guidance for administration of the program to ensure compliance with DOD CIO objectives.

**3.2.2.** Support Contracting Officer Representatives (COR) in identifying IA tasks within a contractor's PWS.

**3.2.3.** Assist USTRANSCOM Directorates in identifying positions assigned to perform IA functions.

**3.2.4.** Provide guidance and support USTRANSCOM Directorates and CORs in accomplishing skill assessments, including on-the-job evaluations.

**3.2.5.** Support reassessment of an individual's skills to perform in an IA position in cases where personnel repeatedly fail to obtain required IA certifications.

**3.2.6.** Provide an appointment letter to personnel in technical category positions, including a statement of responsibilities for the system. For contractor personnel, this letter will be provided to the COR.

**3.3.** TCJ6-I. Ensure reporting of IAWIP statistics as part of FISMA reporting.

**3.4.** USTRANSCOM Directorates and Staff Agencies will:

**3.4.1.** Identify all positions performing IA functions by category and level. This applies to all positions with IA duties, whether performed as primary or additional/embedded duties.

**3.4.2.** Participate in quarterly Certification Requirement Assessments to identify new IA positions.

**3.5.** USTRANSCOM Manpower and Personnel Directorate (TCJ1) will:

**3.5.1.** Update manpower authorizations in the Joint Table of Distribution within USTRANSCOM with appropriate IAWIP coding.

**3.5.2.** Ensure military and civilian positions are filled by qualified personnel or ensure personnel obtain qualifications within required timeframes. Where IAWIP certified personnel cannot be provisioned to fill a valid IAWIP requirement, notify the gaining organization and the IAWIP program manager.

**3.5.3.** Provide information on continuing education opportunities, classes, etc., to support the staff in maintaining their certifications.

**3.5.4.** Coordinate with Civilian Personnel Section, as necessary, regarding civilian personnel who fail to obtain/maintain required IA certifications.

**3.6.** DISA Field Security Operations will assist in identifying and acquiring computing environment certification training, such as CBTs and DISA provided classes.

**3.7.** CORs will:

**3.7.1.** Ensure all IA functions to be performed by contractors and the associated IA certifications, to include computing environment certifications, are included in the contractor's PWS.

**3.7.2.** Validate IA certifications of contractors assigned to perform IA functions prior to start of new task/contract.

**3.7.3.** Review monthly reports to ensure contractors performing IA functions are appropriately certified. If a deviation is identified, contact the IAWIP Functional Program Manager for resolution.

**3.7.4.** Ensure that required on the job evaluations are accomplished by contractors and documentation indicating completion is provided.

**3.8.** Personnel in IAWIP identified positions will:

**3.8.1.** Obtain appropriate IA certification based on category and level identified for position. For military and civilian personnel, request a certification exam voucher from TCJ6, Operations and Plans Division, Information Assurance Branch (TCJ6-OI) in the DOD Personnel Certification Support System.

**3.8.2.** Register in Defense Workforce Certification Application to allow validation of certification status.

**3.8.3.** Ensure that applicable continuing education and certification requirements required to maintain certification are met.

**3.8.4.** Complete Privileged Access Agreement, if required. Privilege Access Agreements may be obtained from the IAWIP Program Manager.

**3.8.5.** As required, obtain appropriate computing environment certifications. For military and civilian personnel, evidence of training completion should be provided to the IAWIP Program Manager. For contractors, evidence of training completion should be provided to the COR.

**3.9.** Supervisors of personnel in IAWIP identified positions will:

**3.9.1.** Ensure that military and civilian IA personnel receive appropriate on-the-job training (OJT).

**3.9.2.** Ensure that an on-the-job evaluation (OJE) is performed prior to military, civilian, and contractor IA personnel receiving privileged access to any system/network device. OJEs must assess a person's ability to execute the functions for which privileged access is required. OJEs need only be performed when personnel are first assigned to the position. OJEs will be accomplished for government personnel by personnel designated by the IAWIP Functional Program Manager and for contractor personnel by personnel designated by the contracting officer.

**3.9.3.** Ensure memorandum (Attachment 2) is submitted to TCJ6-OI for any uncertified personnel performing IA functions under the conditions delineated in paragraph 4.2.

**3.9.4.** Perform actions detailed in section 4.5, as appropriate, regarding military and civilian personnel who fail to obtain required IA certifications.

**3.10.** IAT Level III Supervisors will:

**3.10.1.** Provide OJT for IAT Level I and II DOD personnel.

**3.10.2.** Sign Privileged Access Agreements for IAT Level I and II staff, as required.

**4. Policy**

**4.1.** Assigning personnel. USTRANSCOM vacant military and civilian IA positions should be resourced with appropriately certified personnel. When no appropriately certified candidates exist, newly assigned military and civilian personnel have six months to obtain the appropriate certification applicable to the position to which they are assigned. Military and civilian personnel in newly identified IA positions (reference paragraph 4.6) have six months to obtain appropriate certification. Contractors must possess appropriate IA certification prior to performing any IA functions delineated in DODM 8570.01-M.

**4.2.** Uncertified personnel. Military and civilian personnel within their six month window to obtain certification, may perform the IA functions under direct supervision of an appropriately certified individual. Uncertified personnel performing functions under the supervision of an appropriately certified individual must be documented in a memorandum to the USTRANSCOM Information Assurance Manager. Template for memorandum is provided at Attachment 2.

**4.3.** Computing environment certification. Personnel who have been identified as requiring IAT certification and who have been granted privileged access (i.e., any elevated privilege beyond normal user-level access), must also be certified for the computing environment in which they have privileged access. Attachment 3 provides guidance on obtaining computing environment certification. Additionally, personnel with privileged access must complete a Privileged Access Agreement.

**4.4.** Maintaining certification. It is the individual’s responsibility to know and comply with any continuing education requirements for their specific IA certification. USTRANSCOM will provide information on continuing education opportunities, training classes, etc., to support personnel in maintaining their certifications.

**4.5.** Failure to obtain/maintain certification. Military and civilian personnel who fail to obtain required IA certification, or fail to maintain a required achieved certification, may be reassigned to other duties. Contractors will not perform IA functions until certification is achieved and those who fail to maintain required certification will not be allowed to continue performing IA functions within USTRANSCOM.

Failed Attempt	Result	Responsible Authority	Actions Required
First	Placed in remedial supervised training (CBTs, Advanced Distributed Learning Service, hands-on training) and will not be allowed to perform IA duties	Supervisor	Military/Civilian “Additional Duty” employees: Reassign the IA duties.  Military: Document individual’s training regimen, to include trainee’s understanding of course content, motivation level, and study habits.

	without the direct supervision of an appropriately certified individual		<p>Validate the trainee's readiness for retesting and schedule the person to take the examination within 60 days.</p> <p>Civilians: "Condition of Employment" employees, contact TCJ1 to determine appropriate actions.</p>
Second	Removed from IA position/duties	Supervisor/Division	<p>Military: TCJ6-OI meet with both supervisor and individual to reassess individual's skills to perform in an IA position. Assess individual's aptitude, motivation, experience, and knowledge level to perform in an IA-coded position. Schedule for instructor led training.</p> <p>Civilians: Contact TCJ1 to determine appropriate actions.</p>
Third	Prevented from performing any IA duties	Supervisor/Directorate	<p>Military: Individual must be moved to a position not requiring IA knowledge, skills, and abilities. Individual cannot have privileged access to perform IA functions or responsibility for managing system security.</p> <p>Civilians: Contact TCJ1 to determine appropriate actions.</p>

**4.6. Certification Requirement Assessment.** Quarterly reviews will be performed to ensure that all positions (military, civilian and contractor) assigned to perform IA functions delineated in DODM 8570.01-M are identified and appropriate certification levels are determined. Newly identified military and civilian positions will be provided to TCJ1 for coding in the personnel system. Newly identified contractor positions must be provided to the COR to support contract modification.

EARL D. MATTHEWS  
 Brigadier General, USAF  
 Director, Command, Control, Communications  
 and Computer Systems

## Attachment 1

### GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

#### Section A – References

DOD Manual 8570.01-M, *Information Assurance Workforce Improvement Program*

DOD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management*

USTRANSCOM Instruction 31-11, *USTRANSCOM Security Program*

#### Section B - Abbreviations and Acronyms

CBT – Computer Based Training

COR – Contracting Officer Representative

DISA – Defense Information Systems Agency

DOD – Department of Defense

IA – Information Assurance

IAT – Information Assurance Technical

IAWIP – Information Assurance Workforce Improvement Program

OJE – On the Job Evaluation

OJT – On the Job Training

TCJ1 – USTRANSCOM Manpower and Personnel Directorate

TCJ6 - USTRANSCOM Command, Control, Communications and Computer Systems Directorate

TCJ6-I – TCJ6 Chief Information Office and Distribution Portfolio Management Division

TCJ6-OI –TCJ6, Operations and Plans Division, Information Assurance Branch

USTRANSCOM – United States Transportation Command

#### Section C - Terms

Direct Supervision. Oversight provided by immediate supervisor.

On the Job Training. Supervised, hands-on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

Privileged Access. An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls:

Access to the control functions of the information system/network, administration of user accounts, etc.

Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.

Ability and authority to control and change program files, and other users' access to data.

Direct access to operating system level functions (also called unmediated access) that would permit system controls to be by-passed or changed.

**Attachment 2**  
**MEMORANDUM FOR UNCERTIFIED PERSONNEL PERFORMING INFORMATION**  
**ASSURANCE (IA) FUNCTIONS**

MEMORANDUM FOR USTRANSCOM TCJ6-OI

FROM: Office Symbol

SUBJECT: Designation of Supervisor for Uncertified Personnel Performing IA Functions

1. The following individual has been assigned to perform IA functions within USTRANSCOM. This individual does not currently possess the appropriate IA certification required to perform these functions, but, IAW USTRANSCOM Instruction 33-58, *Information Assurance Workforce Improvement Program*, Section 4.2, is authorized to perform these IA functions under the supervision of the IA certified individual designated below.

Uncertified Individual: *Name*

Organization: *TCJ#-XX*

Required Certification: *DOD 8570.01-M Certification and level (e.g. IAT II)*

Description of IA Functions: *Brief description of IA functions that have been assigned.*

Certified Individual: *Name*

Organization: *TCJ#-XX*

Certification Details: *Certification name and number (e.g. CISSP, 123456)*

2. This memorandum expires six months from the signature date below.

\_\_\_\_\_  
 Signature, Uncertified Individual

\_\_\_\_\_  
 Date

\_\_\_\_\_  
 Signature, Certified Individual

\_\_\_\_\_  
 Date

**Attachment 3**  
**COMPUTING ENVIRONMENT CERTIFICATION GUIDANCE**

Information Assurance Technical (IAT) personnel with privileged access must obtain appropriate Computing Environment (CE) certifications for the operating system (OS) and/or security-related tools/devices supported. Although CE certification for all OS and tools supported is desired, at a minimum, certification is required for the primary OS or tool supported. Note: CE certifications may need to be renewed when a new version of the OS or tool is implemented if the changes are significant.

For USTRANSCOM, the following certificates will be accepted as evidence of CE certification.

Certificates of training awarded from the OS or tool vendor (e.g. Sun certificate for Solaris System Administration training, Microsoft certificate for Windows 2008 System Administration).

Certificates generated upon successful completion of Computer Based Training (e.g., Host Based Security System training).

Certificates of successful course completion awarded by Defense Information Systems Agency Field Security Operations for classroom training.