



Information Assurance Workforce (IAWF) Contracting Officer Representative (COR) & Project Manager (PM) Workshop

Shannon Lawson
Command IAM SSC Pacific

Agenda

- ▼ IAWF Program
- ▼ Background and Purpose
- ▼ IAWF Requirements for Contractor Workforce
- ▼ Roles and Responsibilities
- ▼ IAWF Guidance
- ▼ Summary
- ▼ Supplemental Information
- ▼ Questions / Comments

Information Assurance Workforce (IAWF) Program

▼ IAWF

- It was developed and designed to provide:
 - a DoD IA workforce with a common understanding of the concepts, principles, and applications of IA for each category, specialty, level, and function to enhance protection and availability of DoD information, information systems, and networks.
 - an established baseline for technical and management IA skills among personnel performing IA functions across the DoD enterprise.
 - a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive training, blended training, supervised on the job training (OJT), exercises, and certification/recertification.

Background and Purpose

- ▼ **Background**: The DoD 8570.01-M and DFAR's PGI 239.7102-3 have promulgated that Contractor personnel will have documented current Information Assurance certification status within their contract.
- ▼ **Purpose**: The purpose of this presentation is to provide guidance and instruction for COR's to identify all contractors performing IA functions and align them with the categories and levels and ensure that contractor personnel have the appropriate IA certification and background investigation.

IAWF Requirements for Contractor Workforce

▼ Requirement

- Contractor personnel who are currently assigned to SSC Pacific are now required to meet IAWF standards in order to maintain/ gain privileged access (IAT 1/2/3) on DoD computer systems or perform duties in an IAM 1 level (Information Assurance Officer).
 - As stated in NAVYCYBERFORCES 5239.1, contractor personnel may not hold IAM 3 position and may not hold IAM 2 position unless granted a waiver by NAVYCYBERFORCES.
- ▼ All FY 12 (Oct 1) new contractors MUST be FULLY certified
- ▼ Current contractors performing IA functions will have 6 months to become FULLY certified from Oct 1 in ALL applicable Categories/ Levels/ Operating Environments
 - This has been the requirement since September 30, 2010
- ▼ To be a System Administrator of Record, personnel must be fully certified

COR Role and Responsibilities

- ▼ Work with Project Managers to specify contractor certification requirements are in all contracts that include acquisition of IAWF services;
- ▼ Ensure that contractor personnel, including local nationals, have the appropriate IA certification and background investigation;
- ▼ Modify existing contracts to include certification requirements and condition of employment;
- ▼ Document contractor IA certifications in the Defense Workforce Certification Application (<https://www.dmdc.osd.mil/appj/dwc/index.jsp>)
- ▼ A monthly report will be sent to SSC Pacific IAWF team using the Contractor A/C/D (Add/Change/Delete) form. This will capture all contractor personnel who are require IAWF membership to fulfill their contracted tasks
 - Contracts will verify the information sent to IA

PM Role and Responsibilities

- ▼ Ensure specific IA requirements by Category/ Level/ Operating Environment are explicitly stated in the Performance Work Statement (PWS) by task;
- ▼ Must inform the COR with any changes in contractor personnel or task that impacts IAWF;
 - The COR will send a monthly report to SSC Pacific IAWF team using the Contractor A/C/D form. This will capture all contractor personnel who are require IAWF membership to fulfill their contracted tasks
 - Contracts will verify the information sent to IA
- ▼ Ensure that the certifications and certification status of all contractor personnel performing IA functions are identified, documented and tracked;
- ▼ Ensure that contractor personnel, including local nationals, have the appropriate IA certification and background investigation;
- ▼ Ensure that COR modifies existing contracts to include certification requirements and condition of employment;
 - COR will document contractor IA certifications in the Defense Workforce Certification Application (<https://www.dmdc.osd.mil/appj/dwc/index.jsp>)

Contracts Role and Responsibilities

- ▼ Ensure that a repeatable process is established to identify IAWF tasks and services and that when identified, they are captured and documented into a SOW or PWS; Assist with contract mechanics
- ▼ Ensure that monthly reports that are delivered to SSC Pacific IAWF team by the CORs are accurate in terms of contract/ task order number;
 - If inaccurate, Contracts will work with COR to correct data errors
- ▼ Contracts will continue to partner with Information Assurance to ensure accurate data is captured and that contractor personnel who require membership into IAWF are accounted for
 - Establish joint communications to COR/ PM/ Contractor workforce
 - Establish joint training sessions for COR & PM teams
 - Meet to fix any process issues

Information Assurance Role and Responsibilities

- ▼ Ensure contractors being reported by COR/ PM are being added to IAWF and tracked for compliance;
- ▼ Work with CORs and PMs to ensure appropriate certifications are identified;
- ▼ Ensure that a consolidated monthly report are delivered to SSC Pacific IAWF team by ALL CORs;
 - Ensure report accuracy by sending reports to Contracts for confirmation
 - If inaccurate, Contracts will work with COR to correct data errors
- ▼ Information Assurance will continue to partner with Contracts to ensure accurate data is captured and that contractor personnel who require membership into IAWF are accounted for
 - Establish joint communications to COR/ PM/ Contractor workforce
 - Establish joint training sessions for COR & PM teams
 - Meet to fix any process issues

IAWF GUIDANCE

▼ *Key items to look for to help determine if IAWF should be a factor.*

1. Does the contract require vendors to supply personnel who:

- Install IT hardware, software, networks or security system
- Manage or support IT hardware, software, databases, networks, or security systems.
- Build IT systems or develop software or databases
- Provide Information Assurance (IT security) support or management services

2. **If the answer is YES to any questions in #1 then:**

- Does the PWS clearly define the IAWF functional responsibilities to be performed and the exact IAWF category/ level/ operating environment for each responsibility/task?
- Does the PWS provide the IAWF training, certification, certification maintenance, and sustainment training for each functional responsibility?
- Does the contract detail Contract Delivery Requirements Lists (CDRLs) for the reporting of the IAWF certifications and certification status of all Contractor IAWF?

IAWF GUIDANCE (Cont'd)

- ▼ *Key Words to help determine if IAWF should be a factor.*
 - Privileged Access
 - Ability to log on a Government computer as a Systems Administrator
 - Permission to install, uninstall or modify software/ operating systems
 - Permissions to access and/or modify a database
 - Capability to delete or otherwise modify user accounts on Government systems
 - Perform network scans (e.g., ISS, RETINA)
 - Perform system upgrades or modifications

Summary of COR & PM IAWF Requirements

- ▼ For any Information Technology related task that requires contractor labor, the COR will validate with the Project Manager or Technical POC if IAWF tasks are present.
- ▼ Prior to award, the COR will ensure the PM/TPOC provides in the solicitation:
 - A list of information assurance tasks and functional responsibilities for DoD information systems by category and level and the information assurance training, certification, certification maintenance.
 - Any continuing education or sustainment training required for the contractor information assurance functional responsibilities.
- ▼ Post award, the COR and PM will:
 - Document the current IA certification status of contractor personnel by category and level, in the DWCA.
 - Ensure that the certifications and certification status of all contractor personnel performing IA functions are identified, documented and tracked.
- ▼ The COR will ensure existing contracts are reviewed for IAWF requirements and, if such tasks are present, require a modification to comply with DoD 8570.01-M.

Points of Contact

- ▼ SSC Pacific Command IAM: shannon.lawson@navy.mil
(619) 553-3187
- ▼ Contracts Division Head: sharon.pritchard@navy.mil
(619) 553-4492
- ▼ IAWF Manager: Andrew Smith
ssc_pac_iawf_mgt@navy.mil (619) 767-4587
- ▼ IAWF Training Coordinator: jim.mathis@navy.mil
- ▼ IAWF Blog: <https://blog.spawar.navy.mil/iawf/contracting.html>

Supplemental Information

Sample Language for Basic IDIQ Contract SOW/PWS:

- ▼ All IA functions to be performed under this contract will be identified at the task order level in the performance work statement.
- ▼ Task order performance work statements will specify, as applicable, IA workforce category, level, training, and certification requirements for contractor personnel with privileged access working in
 - IA Technical (IAT) environments,
 - IA Management (IAM) personnel with significant IA tasks,
 - Computer Network Defense Service Providers (CND-SPs), and
 - IA Systems Architects and Engineers (IASAEs).
- ▼ Task orders with IA functions will include a requirement for the contractor to report IA certification status and compliance.

Sample Language for Completion Contract or Delivery Order SOW/PWS:

- ▼ The following IA workforce categories, levels, training, and certifications are required for contractor personnel under this task order: [Identify all IA functions to be performed under this task order including IA workforce category, level, training, and certification requirements for contractor personnel with privileged access working in IA Technical (IAT) environments, IA Management (IAM) personnel with significant IA tasks, Computer Network Defense Service Providers (CND-SPs), and IA Systems Architects and Engineers (IASAEs).]

DFARS PGI 239.7102-3 (1 of 2)

DFARS PGI 239.7102-3 -- 'Information assurance contractor training and certification' requires the COR to document the current IA certification status of contractor personnel by category and level in the Defense Eligibility Enrollment Reporting System** required by the DOD Manual 8570.01-M -- and further that existing contracts be modified to specify contractor training and certification requirements -

(PGI 239.7102-3 copied) -- DFARS PGI 239.7102-3 Information assurance contractor training and certification.

(1) The designated contracting officer's representative will document the current information assurance certification status of contractor personnel by category and level, in the Defense Eligibility Enrollment Reporting System, as required by DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(2) DoD 8570.01-M, paragraphs C3.2.4.8.1 and C4.2.3.7.1, requires modification of existing contracts to specify contractor training and certification requirements, in accordance with the phased implementation plan in Chapter 9 of DoD 8570.01-M. As with all modifications, any change to contract requirements shall be with appropriate consideration.

Per DFARS 239.7102-3 -- after contract award, the requiring activity (code) is responsible for ensuring that the certifications and certification status of all contractor personnel performing IA functions described in the DOD Manual 8570.01-M are in compliance with the manual and are identified, documented and tracked –

(DFARS 239.7102-3 copied) -- DFARS 239.7102-3 Information assurance contractor training and certification.

DFARS PGI 239.7102-3 (2 of 2)

(DFARS 239.7102-3 copied) -- DFARS 239.7102-3 Information assurance contractor training and certification.

(a) For acquisitions that include information assurance functional services for DoD information systems, or that require any appropriately cleared contractor personnel to access a DoD information system to perform contract duties, the requiring activity is responsible for providing to the contracting officer-

(1) A list of information assurance functional responsibilities for DoD information systems by category (e.g., technical or management) and level (e.g., computing environment, network environment, or enclave); and

(2) The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

(b) After contract award, the requiring activity is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.

(c) The responsibilities specified in paragraphs (a) and (b) of this section apply to all DoD information assurance duties supported by a contractor, whether performed full-time or part-time as additional or embedded duties, and when using a DoD contract, or a contract or agreement administered by another agency (e.g., under an interagency agreement).

(d) See PGI 239.7102-3 (Pop-up Window or PGI Viewer Mode) for guidance on documenting and tracking certification status of contractor personnel, and for additional information regarding the requirements of DoD 8570.01-M.

IAM Category

- ▼ **IAM Level I** personnel are responsible for the implementation and operation of a DoD IS or system DoD Component within their Computing Environment. Incumbents ensure that IA related IS are functional and secure within the CE.
- ▼ **IAM Level II** personnel are responsible for the IA program of an IS within the NE. Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the Network Environment.
- ▼ **IAM Level III** personnel are responsible for ensuring that all enclave IS are functional and secure. They determine the enclaves' long term IA systems needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through the DoD certification and accreditation process.

IAT Category

- ▼ **IAT Level I** personnel make the Computing Environment (CE) less vulnerable by correcting flaws and implementing IAT controls in hardware or software installed within their operational systems.
 - In general, IAT1s manage/build desktops & laptops or standalone networks
 - May work on servers for specific tasks, but under the oversight of an IAT2
- ▼ **IAT Level II** personnel provide Network Environment (NE) and advanced level CE support. They pay special attention to intrusion detection, finding and fixing unprotected vulnerabilities.....
 - In general, IAT2s manage/build servers or networks that connect to command level networks (e.g. RDTE, SWAN)
 - May build/manage enclave level systems, but under direction of written guidance or supervision of IAT3 personnel
- ▼ **IAT Level III** personnel focus on the enclave environment and support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments.
 - IAT3 are tasked with determining/controlling the security policies and configurations of enclave (e.g. SIPR, NIPR, DREN, SWAN, RDTE) devices and systems