	Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **JUL 2008**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**	
4. TITLE AND SUBTITLE **Educated and Trained Information Assurance Workforce: Key to Our Mission Success**		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **DoD-CIO Information Assurance Workforce Improvement Program Washington, D.C. 20301-6000**		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**			
13. SUPPLEMENTARY NOTES **CROSSTALK The Journal of Defense Software Engineering July 2008**			
14. ABSTRACT			
15. SUBJECT TERMS			

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**3**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Educated and Trained Information Assurance Workforce: Key to Our Mission Success

George Bieber

Director, Information Assurance Workforce Improvement Program

The article summarizes the DoD's strategic IA workforce objectives, progress made in 2007 toward implementation, and the way ahead in 2008 and beyond.

Just like any organized structure, a highly networked systems environment is only as good as its people. Federal agencies and organizations are unable to protect the integrity, confidentiality, and availability of information without a workforce that is adequately trained and educated in IA. DoDD 8570.1, *IA Training, Certification, and Workforce Management*, and its accompanying IA Workforce Improvement Program (WIP) manual (DoD 8570.01-M), represent the first steps toward building and making professional the IA workforce within the DoD.[1]

The IA WIP implements the requirements of DoDD 8570.1 and establishes the organization's IA WIP policy and procedures. Its initiatives are aligned to the DoD Information Management/IT Strategic Plan. The program's vision is to establish an IA professional workforce with knowledge, skills and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures. Integral to this vision is the ability to effectively manage the IA workforce to place people with the right skills in the right place at the right time.

The foundation to build this capability consists of the following five strategic IA workforce objectives:

1. **Certify the workforce.** Establish baseline certifications across the enterprise and certify the workforce according to those baselines.
2. **Manage the workforce.** Provide the tools to facilitate both component management of its IA workforce and the insight of the OSD into DoD's overall workforce status and certification posture.
3. **Sustain the workforce.** Enable DoD workforce to receive continuous learning opportunities to keep their skills current to combat new network threats.
4. **Extend the discipline.** Infuse IA into professional education programs to expand operational leadership's attention to the domain.
5. **Evaluate the workforce.** Establish a means of assessing compliance and measuring program effectiveness.

Milestones to Success

The 2007 calendar year marked the conclusion of the first year of a four-year implementation plan for the IA WIP. Significant milestones were met throughout the year within each strategic objective area. The following are a few of these important milestones:

- **The DoD met its goal to certify 10 percent of the IA workforce for 2007.** The CIO DIAP, charged with the oversight of the IA WIP, put in place a number of initiatives to assist DoD component IA managers and personnel to achieve this goal including certification self-assessment programs. For example, the International Information Systems Security Certifications Consortium (ISC2) Self Assessment Program for the DoD, provided Certification Information System Security Professional (CISSP) candidates access to practice exam questions that yielded measurable results for students to assess their level of preparedness. Self-assessment programs are also available for students seeking Global Information Assurance Certification, Information Systems Audit and Control Association, and Computing Technology Industry Association certifications.
- **The CIO DIAP put the enterprise-wide concept into practice by developing and conducting a certification voucher program on behalf of the DoD components (known as the Voucher Pilot Program).** Personnel certification requirements were gathered from the components and coordinated with commercial certification providers in the form of bulk voucher purchases. The Personnel Certification Support System (PCSS), an online voucher management system, maintained all voucher allocation and distribution information for each component. The PCSS will continue to be used for the second year of implementation as an effective tool to manage certification vouchers.
- **Upgrades to the Defense Civilian Personnel Data System (DCPDS) are complete and the IA personnel data entry process is under way.** Components must now enter all relevant civilian IA workforce data into the DCPDS including IA positions held and appropriate training and certification requirements. This milestone achievement brings components a step closer to more effective civilian workforce management. Increased workforce management provides leadership with assurance that qualified IA personnel are filling IA positions.
- **The Defense Federal Acquisition Regulation Supplement (DFARS) required by DoD Directive 8570.1 is officially approved and can be used in new solicitations and resulting contracts.** The new clause was published in the January 10, 2008 issue of the Federal Register. The announcement included actual wording for the clause regarding IA contractor training certification. DFARS guidance instructs that any modifications to existing contracts will have to be negotiated with the contractor.[2]
- **DISA-supported enhancements of the Carnegie Mellon University developed Virtual Training Environment (VTE) to provide training to meet DoDD 8570 requirements.** The CIO DIAP has funded specific training and lab capabilities for this program, making it available at no cost to 10 percent of DoD personnel in 2007. The VTE is a resource to DoD employees for information assurance, incident response and computer forensic training, with close to 600 hours of materials available. The environment delivers classroom instruction and self-paced online training for CompTIA security+ and ISC2 CISSP to name a few. Seven DoD 8570.01-M role-based optional courses are currently available for personnel. Additional training courses will be offered in the near future.

• **In fiscal year 2007, 29 students graduated from the program and are currently working full time in IA strategic positions across the DoD. The DoD IA scholarship program awarded 269 scholarships to students seeking bachelor's, master's and doctorate degrees in IA fields of study since the program's inception in 2001.** The DoD IA Scholarship Program (IASP) awarded 269 scholarships. In fiscal year 2007, 29 students graduated. The IASP provides educational incentives to foster the recruitment and retention of qualified IA/IT personnel. As a resource for DoD IA professionals to continuously enhance their skills and to keep current with technology and threats, the IASP supports the IA WIP strategic objective to sustain the workforce.[3]

Monitor Success

As the message about the IA WIP program disseminates across the DoD, the goals become more rigorous and the mission more clear. The second year (2008) of the program's implementation includes the following new challenging milestones:

• By the end of 2008, 40 percent of the DoD workforce must be certified according to DoD 8570.01-M baseline policy requirements.

• New specialty positions were proposed for integration into a second change to the 8570.01-M including C&A and software application developers. SME working groups will be organized to focus on the strategy and planning to execute these proposed changes.

• The strategic IA workforce objective, *Evaluate the Workforce*, will play a greater role in program activities. The first IA WIP site review will be conducted in the first quarter of 2008. The intent of these site reviews is to verify DoD component compliance with requirements of DoDD 8570.1 and 8570.01-M. Furthermore, on-site inspections provide the opportunity for the DIAP to assess the level of effectiveness of the IA WIP at the operational level.

Achieve Success

Ultimately, the DIAP seeks to foster continued improvement throughout each year of the program's lifecycle. The implementation planning strategy of the IA WIP dictates a continuous cycle of milestone achievement, benefits actualization, oversight, and improvement. Adherence to this planning strategy will result in a better trained, certified, and professional DoD IA workforce. Results will yield a more capable workforce – and the more capable the workforce, the more likely it is to achieve DoD mission success.◆

Notes
1. Supporting documents can be found at <www.whs.mil>.
2. The full guidance can be found at <www.acq.osd.mil/dpap/dars/dfars pgi/current/index.html>.
3. More information about the IASP can be found at <www.defenselink.mil/cio-nii/iasp>.
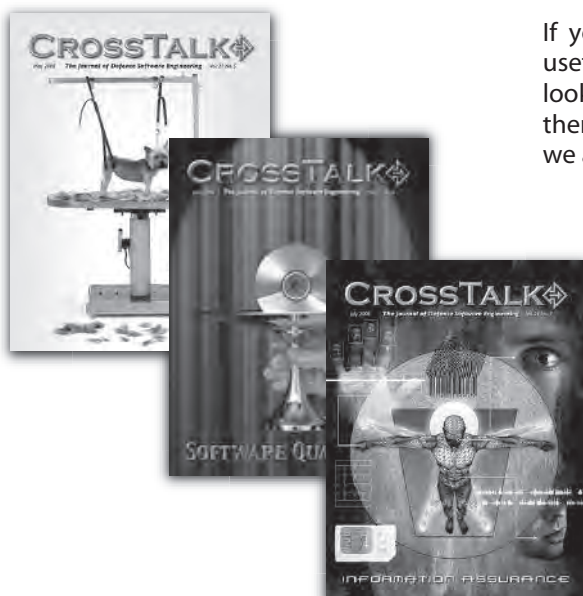
About the Author

George Bieber is the Director of the IA WIP program under the DoD CIO. He oversees implementation of the DoD IA WIP, the DoD IASP, and the DoD Shared Service Center for Tier 1 Security Awareness Training under the Office of Management and Budget-mandated Information System Security Line of Business. Bieber served on the President's Critical Infrastructure Protection Board Education Standing Committee, and is a past executive board member of the Federal Information System Security Educators Association. He currently serves on the American National Standards Institute Personnel Certification Accreditation Committee.

Phone: (703) 602-9980
E-mail: george.bieber@osd.mil

CALL FOR ARTICLES

If your experience or research has produced information that could be useful to others, CROSSTALK can get the word out. We are specifically looking for articles on software-related topics to supplement upcoming theme issues. Below is the submittal schedule for three areas of emphasis we are looking for:

Software Measurement
February 2009
Submission Deadline: September 12, 2008

Software as a Service
March 2009
Submission Deadline: October 17, 2008

Web-Enabling Applications
April 2009
Submission Deadline: November 14, 2008

Please follow the Author Guidelines for CROSSTALK, available on the Internet at <www.stsc.hill.af.mil/crosstalk>. We accept article submissions on software-related topics at any time, along with Letters to the Editor and BACKTALK. We also provide a link to each monthly theme, giving greater detail on the types of articles we're looking for at <www.stsc.hill.af.mil/crosstalk/theme.html>.

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government