



# DIACAP Dimensions

Volume 5 Issue 1 • January 2011

DIACAP Resource Center • www.diacap.net • Email: diacap@diacap.net • Phone: (540) 808-1050 • Fax: (540) 808-1051

## C&A Transformation The Saga Continues....

By Lon Berman

In several past issues of *DIACAP Dimensions* we've reported on the ongoing effort among DoD, the Intelligence Community, and the "civilian" Federal agencies (e.g., Dept. of State, Homeland Security, Justice, Treasury, etc.) to develop and deploy a unified Certification and Accreditation process. A unified C&A process will foster "trust" among system owners in diverse elements of the federal space, thus facilitating interconnection and information sharing. As a citizen and taxpayer I would certainly welcome this small step towards efficiency in government. As an information assurance professional, I can only say "it's about time!"

The Joint Task Force Transformation Initiative (JTFTI), a committee with membership across all three segments of the executive branch (DoD, intelligence, and civil), was formed

with the express purpose of developing the unified C&A process and publishing the guidance documents necessary to implement it. Under the leadership of the National Institutes for Standards and Technology (NIST), JTFTI has produced a series of publications documenting a Risk Management Framework (RMF) for security of information systems throughout their life cycle.

NIST Special Publication (SP) 800-37, Revision 1, presents the roles, responsibilities, and life cycle process steps of the RMF. It is roughly equivalent to DoD Instruction 8510.01, commonly known as the "DIACAP Instruction". NIST SP 800-53, Revision 3, presents a catalog of "Security Controls" that are similar, albeit more comprehensive, than the IA Controls presented in DoD Instruction 8500.2, "Information Assurance Imple-

mentation."

It is a virtual certainty that DoD will adopt the RMF, and the NIST Security Controls that go with it, at some point. Thus far, however, there has been no definitive policy or guidance from DoD. That is not to say there has been no progress at all, however. DoD has now established a "C&A Transformation" page on the DIACAP Knowledge Service. Only some rudimentary information is currently published there, but more is promised in the near future.

What sort of transformation information has DoD released? A short Frequently Asked Questions (FAQ) section assures us the transformation will be gradual, so there is no cause for alarm. It also informs us provisions will be made for systems already approved under the existing DIACAP, so, again, no need to push the

See C&A on page 3

## Not Applicable — Is it applicable to YOU?

By Kathryn Farrish

According to DoDI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), identifying applicable IA controls for an information system is a critical activity in the DIACAP. First, it is important to identify the baseline IA controls, which are the

minimum set of IA controls that must be addressed to achieve adequate security for an IS. Baseline IA controls are prescribed in the DoDI 8500.2, IA Implementation, based on the MAC and CL.

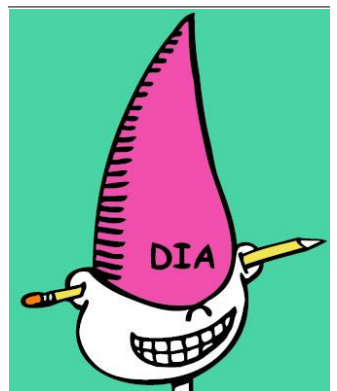
It is also necessary to determine with IA controls are not applicable (NA) for your infor-

mation system. NA IA controls are those that do not impact the IA posture of the IS as determined by the Designated Approving Authority (DAA). Now, don't think the DAA will go through the controls and determine which ones are applicable himself. The DIACAP team will need to determine

See Not Applicable on page 3

### Inside this issue:

<i>C&amp;A Transformation</i>	1
<i>Not Applicable — Is it applicable to YOU?</i>	1
<i>IA Control Spotlight—IA Training</i>	2
<i>Top Ten List—Certifications</i>	2
<i>Don't Forget About the People</i>	4
<i>DIACAP Training Schedule</i>	5



## IA Control Spotlight—Information Assurance Training

By Kathryn Farrish



Spotlight on Information Assurance Training

PRTN-1— “A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery.”

In order to maintain an adequate security posture, organizations need to be diligent in the training of personnel who fulfill IA roles (system administrator, network administrator, information assurance security officer, information assurance manager, etc). The department of defense has published the DoD 8570.01m, The DoD Information Assurance Workforce Improvement Program, to assist organizations in developing their own training

program for personnel. DoD 8570.M categorizes roles for IA personnel based on their interaction with the system and details the minimum training requirements for those personnel. DISA provides free online training through their website to cover basic IA concepts. Many of them are available to both government and contractor personnel (no CAC authentication required). These courses can be located at <http://iase.disa.mil/eta/index.html#onlinetraining>. In addition to online courses, various IA roles require industry accepted, professional certifications such as Comptia’s Security+ the and ISC<sup>2</sup> CISSP (Certified Information System Security Professional). Although there are several other options to fulfill the certifica-

tion requirement, these two are the most popular based on the content covered.

It’s important that an organization implement training requirements within their personnel security policies, or in other applicable documentation. These policies should specify which certifications listed in the DoD 8750.01 they support, which online courses each personnel is responsible for completing and the frequency. While many certifications have no requirement for recertification after a set period of time, it is required that personnel (including desktop users) complete the annual IA refresher course on an annual basis. For more information on industry certifications available, see the article below, “Top Ten — Professional Security Certifications.”

1. CISSP
2. CISM
3. GIAC
4. CISA
5. CSFA
6. CEH
7. CBCP
8. CPP
9. CCE
10. Vender Certifications

## Top Ten List — Professional Security Certifications

By Kathryn Farrish

10. **Vendor Certifications -** CISCO and Microsoft specific certifications top the list as the demand for technical and hands-on professionals increase within organizations.
9. **CCE-Certified Computer Examiner -** Certified Computer Examiner is a certification provided by the International Society of Computer Forensic Examiners (ISFCE). This certification focus’s to increase the level of professionalism and further the field of science and computer forensics. The foundation of this certification maintains a fair, uncompromised process for certifying the competency of forensic computer examiners and sets high forensic and ethical standards for forensic computer examiners.
8. **CPP—Certified Protection Professional -** Certified Protection Professional is a designation for individuals who have demonstrated competency in all areas constituting security management. As the emphasis on protecting people, property, and information increases, it

has strengthened the demand for professional managers, to meet these needs. The ASIS International administers the Certified Protection Professional Program.

7. **CBCP-Certified Business Continuity Professional-** Certified Business Continuity Professional is another specialization gaining prominence within information security, with the outbreak of H1N1 pandemic and with organizations increasingly focusing their efforts in effective crises management and business continuity planning efforts. The CBCP certification offers competency on business continuity and disaster recovery planning responsibilities and accomplishments.
6. **CEH-Certified Ethical Hacker -** Certified Ethical Hacker is another certification gaining popularity as hacking and fraud activities are on the upswing. The CEH program certifies individuals in the specific network security discipline of Ethical Hacking from a vender-neutral perspective. The CEH certification fortifies the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker



Top Ten Professional Security Certifications

## C&A (cont. from page 1)

panic button.

Along with the FAQ, DoD has also produced three notional “mappings” of DIACAP to RMF. There is a mapping of DIACAP activities to RMF process steps, a mapping of roles and responsibilities between DIACAP and RMF, and a mapping of DoDI 8500.2 IA Controls to NIST SP 800-53 security controls. Each of these mappings comes with a prominent disclaimer that it is preliminary and “for reference only.” Still, there *is* some cause for concern. The authors of the control mapping were only able

to find corresponding DoD IA Controls for about *half* of the NIST Security Controls. That seems to indicate a difficult road will be ahead of us when it finally comes time to begin the transformation in earnest. Also, the mapping of roles and responsibilities tells us we may need to start learning some new names for old friends, e.g., “Authorizing Official (AO)” instead of “Designated Approving Authority (DAA).”

Here are some suggestions on how to keep up with the ongoing “C&A Transformation” saga:

Monitor the “C&A Transformation” page on the DIACAP Knowledge Service (<https://diacap.iaportal.navy.mil>)

Monitor the “FISMA Implementation Project” section of the NIST website (<http://csrc.nist.gov/groups/SMA/fisma>)

Watch this space - upcoming issues of *DIACAP Dimensions* will provide updates as DoD policy and guidance unfold



**Check out the DIACAP Resource Center for online discussion of important IA topics, training schedules, and new, exciting information regarding the C&A Transformation!**



Remember to have the DAA sign off on all NA controls in either a digitally signed email, or a signed memo. This concurrence should be submitted with your DIACAP package.

## Not Applicable (cont. from page 1)

what is or isn't applicable and then seek formal acknowledgment from the DAA in the form of a digitally signed email or a memo. What is, or is not applicable, will depend on what is inside the accreditation boundary, the information system type, classification level, etc.

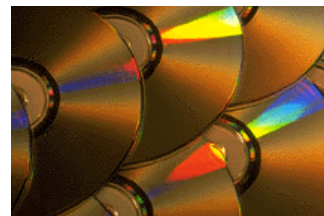
For example, IA control PESL-1 (Screen Lock) may be NA if there are no workstations or servers with attached monitors in the accreditation boundary. EBCR-1 (Connection Rules) would be NA for a stand-alone IS, since it does not connect to anything outside its accredita-

tion boundary. DCMC-1 (Mobile Code) would be NA if the software application does not utilize mobile code technologies such as Java or ActiveX.

Remember, if an IA control is NA, it must be listed as such in the DIACAP Implementation Plan (DIP), Scorecard and in the Plan of Actions and Milestones (POA&M). The POA&M should also include the reason or justification why the control is not applicable. Including NA controls on the POA&M facilitates periodic review to ensure that the circumstances that made them NA

have not changed.

Once it comes time for the Certification, the DIACAP Validator (AKA certification agent) will review the justification. In most cases, the control will simply be marked NA in the scorecard – no testing will be conducted. If the validator takes issue with the NA status this should thoroughly be discussed between the validator and the DIACAP team (including, potentially, the DAA him/herself).





## Don't forget about the People C&A Transition in the Real World Rob Lee, CISSP-ISSEP, CAP

### Meet Rob Lee!

Mr. Lee has over 23 years of professional experience in network operations, information assurance/security, technical client service, and program management. This includes extensive experience in network design, certification & accreditation, security vulnerability assessments, operations and maintenance, information technology infrastructure library (ITIL) implementation, Public Key Infrastructure (PKI), HSPD-12 integration, and defense weapons systems support. Mr. Lee has designed and implemented training curriculum's for technical staff and end users. Mr. Lee has experience in technical project management, and customer relationship management (CRM). Mr. Lee has a proven track record of building and supporting highly motivated and successful customer service teams. Mr. Lee is highly skilled and experienced in exceeding customer expectations. Mr. Lee serves as a Subject Matter Expert in Certification & Accreditation and facilitates instruction in both the DoD Information Assurance Certification & Accreditation Process (DIACAP), and the NIST based Federal C&A Process. Mr. Lee is a Veteran of the United States Army, serves as a member of the Advisory Council for the Computer Security Institute (CSI) and is a member of ISC2, he also holds the credentials of CISSP, ISSEP, and CAP.

The Security Authorization Process (formerly known as the Certification & Accreditation (C&A) process has kept lock and step with Federal Policies, and Guidelines for the protection of Information Systems that process and store critical data. What does all of this mean for Information Assurance (IA) Professionals with the responsibility of determining and reporting the security posture of Information Systems? I'm glad you ask. Within the last year or so, a number of documents, guidelines and procedures have been released and socialized with the intent of transitioning towards a federated process for Security Authorization of Federal Information Systems. IA Professionals now have a wider threat vector to protect their systems against. Advances in commercial building technologies for one, have introduced threats and vulnerabilities related to building control systems, i.e., HVAC, lighting systems and other facility related control systems. New technologies and its implementation, breed new processes, which almost always have an adverse affect on the people who use, maintain and operate these systems. Whether or not you are responsible for the Department of Defense Certification and Accreditation Process (DIACAP) or the Federal version, using the Risk Management Framework (RMF) for Security Authorization. The approach and methodology are the same for each process. The IA professional must ensure that with all the media and publicity associated with security, that there are simple people focused processes that will help engage the users and the implementers of security within their organizations. Information Practitioners should focus on the people, and not as much on the technology.

Often enough, an Information Assurance Professional will find that they have been "VOLUNTOLD", and handed the responsibility for providing security authorization for a system within their program/project area. The expectation is that the individual will be responsible for all events, meetings, contracts, documents, statements of work, disasters, both natural and man-made when it comes to the C&A of the Information System. This process has been the swift introduction into IA for a number of people. I believe that to be effective as an IA Professional one must focus on the people. Spend time building valuable relationships with individuals across the enterprise. Research and determine the expectation of the Designated Approving Authority (DAA). Spend time with the System Owner or Program Manager to let them know that you understand the process and that you are committed to a success-

ful system Security Authorization. Get to know the facilities manager and find out what their hot issues are. Will his or her shop be responsible for implementation of the Homeland Security Presidential Directive (HSPD)-12 ?, which is the implementation of a Personal Identity Verification (PIV) solution that issues Common Access Cards embedded with personal information, system data and individual biometrics, to employees and contractors. Most facilities managers were born as military police officers, than morphed into personnel or facilities security officers, who are now burdened with the implementation of technology. This is fertile ground for developing and building relationships. If you have a background in information technology, or networking, you can provide vital information to your colleagues who are responsible for managing the facility in which your systems may operate. Volunteer to attend meetings with them, vet contractors and vendors who are vying for their time to either sell a system or service. Help them to understand the impact of such systems or services based on your experiences. All the while you are building and developing a trusted relationship which you will need when it comes to collecting artifacts, and scheduling meetings with personnel from their particular program areas. Exercise the same diligence as you build and develop relationships across other areas of the enterprise, i.e., network administrators, database and development groups will all play a role in the collection of data and evidence used to authorize the operation of information systems.

Good IA professionals are also evangelists, who carry a message of acceptance and buy-in of information assurance and the security authorization process. If your introduction to Information Security was through the democratic process of being "VOLUNTOLD", then consider that the same may hold true for your colleagues across the enterprise. Use awareness as a tool to garner support across the enterprise. Perhaps you can start a security workgroup if there is not one already established. Hold monthly meetings to discuss various issues related to security and their implementation into the environment. The more information that you share within your organization, the easier it will be when it comes to understanding and supporting the security authorization of information systems within your environment. Remember; Don't forget about the People.

## DIACAP Training Schedule

DIACAP Resource Center offers *DIACAP Fundamentals* (one-day) and *DIACAP In-Depth* (three-day) classes on a regularly scheduled basis in the National Capital Region, Colorado Springs, Huntsville, and San Antonio and Washington, DC.

Regularly scheduled classes for the calendar year for 2011 are as follows:

DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
7 February 2011 (NCR)	8-10 February 2011 (NCR)
28 February 2011 (SA)	1-3 March 2011 (SA)
7 March 2011 (DC)	8-10 March 2011 (DC)
21 March 2011 (H)	22-24 March 2011 (H)
28 March 2011 (CS)	29-31 March 2011 (CS)
18 April 2011 (NCR)	19-21 April 2011 (NCR)
6 June 2011 (H)	7-9 June 2011 (H)
13 June 2011 (CS)	14-16 June 2011 (CS)
27 June 2011 (NCR)	28-30 June 2011 (NCR)

(NCR) = National Capital Region  
 (CS) = Colorado Springs (H) = Huntsville  
 (SA) = San Antonio (DC) = Washington, DC

For Customers in other locations or those with specific scheduling requirements, we offer the option of “on-site” training. All you need is a group of students (at least 8-10) and a suitable classroom facility. We offer a discount over the normal “per student” registration cost; the discount grows larger as the class size increases. Our “on-site” training fee includes all instructional services, training materials, and instructor travel expenses. Most importantly, you will avoid the travel expenses associated with sending your people to training away from the office. Please contact the DIACAP Resource Center at (540) 808-1050 or [diacap@diacap.net](mailto:diacap@diacap.net) to request an on-site training quotation.

On-line registration and payment for all scheduled classes is available at our website [www.diacap.net](http://www.diacap.net). Registration can also be done by downloading a registration form and submitting the completed form by FAX or email. Payment arrangements include credit cards, SF182 forms, or purchase orders.

Please visit [www.diacap.net](http://www.diacap.net) for the latest training schedule, including any new dates or locations.

## FISMA Risk Management Training

Training is also available in the FISMA (NIST) Risk Management Framework (C&A process) that is used by federal civilian agencies and the intelligence community. This process forms the basis of the forthcoming “unified”, government-wide, Security Authorization process. For information on this training program, please visit [www.fisma1.net](http://www.fisma1.net) or [www.fedca.org](http://www.fedca.org).

## Top Ten (cont. from page 2)

is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker..

### 5. CSFA-CyberSecurity Forensic Analyst -

CyberSecurity Forensic Analyst is an emerging certification and skill within information security getting popular with increased cyber crimes and fraud taking place within an organization. Possessing the CSFA certification is proof that the analyst can conduct a thorough and sound forensic examination of a computer system and other digital/electronic devices, properly interpret the evidence, and communicate the examination results effectively and understandably. The CSFA designation is held exclusively by the most qualified digital forensic professionals and is a testament that the holder has the necessary skills to perform a comprehensive analysis within a limited time frame.

### 4. CISA-Certified Information Systems Auditor -

Certified Information Systems Auditor designation demonstrates proficiency in information security audit, control and security skills. CISA has become a preferred certification program by individuals and organizations around the world. CISA certification signifies commitment to serving an organization and the IS audit, control and security industry with distinction.

### 3. GIAC-The Global Information Assurance Certification -

The Global Information Assurance Certification validates the real-world skills of IT security professionals. GIAC currently offers certifications for over 20 job-specific responsibilities that reflect the current practice of information security including digital forensics, intrusion

and incident handling, security administration, management, operations, legal, audit and software security. The demand for GIAC certifications is increasing as organizations today is driving the need for hands-on-technical personnel.

### 2. CISM-Certified Information Security Manager-

Certified Information Security Manager certification is offered by ISACA and is developed specifically for experienced information security managers and those who have information security management responsibilities. The CISM certification is for the individual who manages, designs, oversees and/or assesses an enterprise’s information security (IS). The CISM certification promotes international practices and provides executive management with assurance that those earning the CISM certification have the required experience and knowledge to provide effective security management and consulting services.

### 1. CISSP—Certified Information System Security Professional

Certified Information Systems Security Professional offered by ISC2 is generally the most recognized internationally and popular with information security professionals. For security practitioners planning to build a career in information security and holding at least five full years of experience in information security, the CISSP credential is an ideal career goal. Increasingly recruiters look for this credential in potential candidates as a validation of their commitment toward this profession.