

Transforming IA Certification and Accreditation Across the National Security Community

Eustace D. King
OASD(NII)/DoD CIO

The IA C&A transformation is a partnership that stretches across the DoD, DNI, CNSS, National Institute of Science and Technology (NIST), and the Office of Management and Budget. Much progress has been made since the DoD and DNI CIOs published an initial set of transformation goals in January 2007; however, much work remains. While core transformational documents are being authored through the CNSS and NIST, many of their underlying transformational concepts are being implemented in the DoD through the new DIACAP and in the intelligence community through the near-final IC Directive 503.

The C&A transformation is actually part of a larger transformation. Within the DoD, this transformation is centered on net-centric operations as set forth in the National Military Strategy¹ with the GIG as a critical enabler. Within the IC, it is centered on a drive toward integration, customer service, and advances in analytic capability.

What is common across the DoD and the IC is the need to leverage the power of information through sharing and collaboration. This means ensuring that useful, understandable information is visible and available where it is needed, when it is needed, and to those who need it. It also means that users and entities acting on their behalf (e.g., software services) can connect and partner to generate new knowledge, get work done, or conduct net-enabled operations.

Because the way the national security community creates and uses information is changing, it must change the way it

builds networks, provisions services, and manages data. In turn, it must change the way it works together to *identify, validate, authorize, manage, and sustain IA capabilities*, which are the objectives of C&A².

Thus, the C&A transformation is about changing the way the national security community manages IA risk. This means breaking down unnecessary barriers between community members and improving information sharing among the security, IT provider, and IT user communities. C&A originated during the days when a few, large standalone mainframes with custom code were typical, and a *steady state* with quantifiable residual risk was expected. The national security community is transforming to service-centric, globally interconnected information enterprises constructed largely from commercially acquired general purpose IT. The legacy, system-centric practice of C&A hinders information sharing and blocks the timely delivery of mission-critical systems.

What Is the Status of the C&A Transformation?

While the C&A transformation was initiated by and remains under the joint sponsorship of the DoD and DNI CIOs, key partners include the CNSS, particularly the C&A working group, and the NIST, particularly the computer security division. The engagement and sponsorship of the CNSS allows key policies and guidelines to be developed and published for a broader community: all federal departments and agencies with NSS. Engagement with NIST allows for synchronization of concepts, standards, and guidelines across both NSS and non-NSS. Some of these documents are currently under formal community review in the CNSS; others are still in the drafting stage (Table 1). Other supporting activities, including transition planning and training, are ongoing.

Transition may vary in time and manner across the national security community. Some organizations are planning to follow the C&A transformation process and doctrine even while documents are going through final review. Others may wait until the authoring process is completed, which is expected to occur around the end of calendar year 2008. Readers must look to each department's or agency's policy issuance for these details. For example, the IC's transition details are being promulgated in IC Directive 503 and supporting issuance whereas the DoD's transition details are being promulgated in the DoD 8500 series, primarily the new DoD Instruction (DoDI) 8510.01, the online DIACAP knowledge service³, and an upcoming revision of DoDI 8500.2.

What Are the C&A Transformation Goals?

In January 2007, the DoD and DNI CIOs published seven goals for transforming C&A processes across the DoD and the IC. The following are the original seven

Table 1: NSS Documents Currently Under Formal Community Review

Document	Purpose	Status
CNSSP 22	Establishes a national risk management policy for national security systems.	Under formal review by CNSS
CNSSI 1199	Establishes the way the national security community categorizes information and information systems with regard to confidentiality, integrity, and availability.	Under formal review by CNSS
CNSSI 1253, aka Security Controls Catalog	Consolidates DCID 6/3, DOD Instruction 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls.	Under formal review by CNSS
CNSSI 1253A	Provides methodology for assessing adequacy of each security control, e.g., testing.	In progress
CNSSI 1260	Provides guidance to organizations with the characterization of their information and information systems.	In progress
Next Generation NIST 800-37	Defines the C&A process (joint DNI, DoD, NIST activity).	In progress

goals along with some implementation details. While the DoD-IC partnership is highlighted, the expectation is that many of the outcomes and benefits described will be realized across the greater national security community and between NSS and non-NSS.

1. **Define a common set of impact levels and adopt and apply them across the DoD and IC.** These are being defined in the new CNSS Instruction (CNSSI) 1199 with consideration for the authorities, complexities, classification needs, and special risks inherent in the national security community.
2. **Adopt reciprocity as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.** Commonly recognized types of national security information and systems are being described in the new CNSSI 1260. These will be supported by reciprocity profiles, tailored sets of security controls for sharing specific types of national security information or systems. Commonly recognized types of information and systems with associated reciprocity profiles will provide agreement on security objectives. Common security controls and assessment methods will provide transparency of security implementation.
3. **Define, document, and adopt common security controls, using NIST SP 800-53 as a baseline.** The new CNSSI 1253 is a comprehensive information system security controls catalog that starts with NIST Strategic Plan 800-53 and normalizes and consolidates the controls from DoDI 8500.2, DCID 6/3, the UCDMO, and CNSS policies (for example, CNSS Policy 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions*), as well as new controls developed through research related to emerging topics such as outsourcing, supply chain risk, and service-oriented architecture. The new CNSSI 1253A is a companion document that provides common assessment objectives (i.e., expected results) and methods for the common controls.
4. **Adopt a common lexicon, using CNSSI 4009 as a baseline, thereby providing both the DoD and IC a common language and common understanding.** The new CNSSI 4009 will serve as a shared dictionary.
5. **Institute a senior risk executive function, which bases decisions on**

an enterprise view of risk considering all factors, including mission, IT, budget, and security. The previous DoD C&A process was intended to balance mission, program, and security risk, but the horizon was local, not enterprise. Today's complex, many-to-many relationships among missions, business functions, and supporting information systems require a holistic, enterprise-wide view to managing risks. The DoD is implementing this goal via the DIACAP governance structure established in DoDI 8510.01. The DIACAP governance structure establishes C&A roles and responsibilities and collaboration mechanisms at every organizational level, from GIG mission areas to heads of components and their chief information officers to individual system program managers, developers, and operators. This comprehensive governance structure is intended to establish a relationship between aggregated information security risks and organizational or enterprise mission and business risks while helping individuals with responsibilities for system implementation and operations to better understand how the information security issues associated with their systems translate into organizational or enterprise security concerns. Over time, the DoD expects to continue to improve this structure and strengthen its interfaces with IC governance structures. Additionally, as part of the next generation 800-37, the DoD is working with NIST and the DNI to address C&A processes for federated enterprises, i.e., for systems and services that span departments and agencies, coalitions, or international strategic partners

6. **Incorporate IA into enterprise architectures and deliver IA as common enterprise services across the DoD and IC.** The DoD is implementing this goal via the IA component of the GIG integrated architecture, a new alignment framework for GIG IA, and a suite of IA capabilities and services being realized through the GIAP.
7. **Enable a common adaptable process that incorporates security within the lifecycle processes and eliminates security-specific processes.** The DoD is implementing this goal via continued integration of IA into the Joint Capabilities Identification and Development System⁴. Who is responsible for coordinating the DoD's participation in the C&A trans-

formation?

- CIO-to-CIO Relations: Gus Guissanie, Principal Deputy, DASD(IIA).
- C&A Operations: Eustace King, DIACAP Program Manager.
- DoD IA Policy: Don Jones, Senior Policy Advisor.

Special Thanks

With input from Sharon Ehlers, Office of the Associate Director of National Intelligence and CIO, and Ron Ross, Computer Security Division, IT Laboratory, NIST.♦

Notes

1. An unclassified version is available at <www.defenselink.mil/news/Mar2005/d20050318nms.pdf>.
2. For example, see the DIACAP definition in DoDI 8510.01, Nov. 2007 <www.dtic.mil/whs/directives/corres/ins1.html>.
3. <<https://diacap.iaportal.navy.mil>>.
4. Chairman of the Joint Chiefs of Staff Instruction 3170.01F. 1 May 2007 <www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf>; the Defense Acquisition System (DoDD 5000.1), and related issuance, <<https://akss.dau.mil/dapc/index.aspx>>; and NetOps <www.stsc.hill.af.mil/CrossTalk/2007/07/0707Lam.html>.

About the Author

Eustace D. King is assigned to the Office of the DASD(IIA). As the principle authority within OSD(NII) IAD for ensuring successful implementation of the DIACAP, King provides oversight and community outreach to ensure understanding and adherence to DIACAP policy vis-à-vis DoDI 8500.2, IA implementation. King is also responsible for fielding and ensuring enterprise-wide training for the Enterprise Mission Assurance Support Service, and management of the DIACAP Knowledge Service. He co-chairs the CNSS Subcommittee, providing leadership to the federal community to aggregately embed IA principles and services within NSS. King retired from the Air Force in 2000.

DASD/IIA-DIAP

Phone: (703) 602-5044

Fax: (703) 602-7209

E-mail: eustace.king@osd.mil

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