OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PUBLIC AFFAIRS OFFICE
WASHINGTON, D.C.
20511

NEWS RELEASE

FOR IMMEDIATE RELEASE
MARCH 27, 2007

ODNI News Release No. 10-07

DNI & DoD Chief Information Officers Announce Certification and Accreditation Transformation Goals

The Associate Director of National Intelligence and Chief Information Officer, Hon. Dale Meyerrose, along with the Department of Defense's Chief Information Officer, Hon. John Grimes, have publicly announced seven Certification and Accreditation (C&A) Transformation goals for both the Intelligence Community (IC) and the Department of Defense (DoD). The proposed changes now underway will strengthen the ability for the Intelligence Community and DoD to more rapidly deploy information technology (IT) systems enabling information sharing between and with others. C&A transformation will drive decision-making based on sound risk management principles, incorporate security into common lifecycles that are approved and used by all DoD/IC enterprises, and eliminate wasteful and redundant processes and paperwork.

"We need to establish a community environment, across security domains, equipped with standard enterprise services and universal data access," said Mr. Meyerrose.

"Certainly the most change will result from the actions we take to reduce redundant activity, unnecessary documentation and shorten the overall process," said Mr. Grimes.

Certification and Accreditation Transformation will be accomplished under seven transformation goals. These changes correct long-standing problems relating to the extensive resources the IC and DoD historically expend, and will help deliver systems to the customer faster.

This announcement finalizes an intense eight-month effort actively involving industry, contractors, academia, IC agencies, DoD, the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and Commonwealth Partners. The seven C&A Transformation goals are:

- Reduce the varying numbers of IC Protection Levels and DoD Mission Assurance Categories (MAC) by defining a ***common set of trust levels*** the IC and DoD can jointly apply to systems eliminating conflicting criteria used to apply security controls that currently inhibit systems' interconnection and information sharing.

- Adopt ***reciprocity***, in the sense of cooperation, as normal business rather the exception to facilitate re-use of systems developed and approved by other organizations. This transformation will reduce duplicative expenditures on multiple systems development efforts.

- Define ***common security controls***, using NIST Special Publication 800-53 as a starting point, enabling the IC and DoD to develop systems to the same protection standards. In doing so, this facilitates reciprocity of approvals and reuse of systems across the IC and DoD communities.

- Define a ***common lexicon*** (common language and common understanding), using the Committee on National Security Systems (CNSS) 4009 glossary as a baseline, for establishing reuse and reciprocity across the IC and DoD.

- Look broader than individual systems or events when making risk decisions. Therefore, implement a ***senior risk executive function*** to base decisions on ***an "enterprise" view of risk considering all factors***, including mission, IT, budget, and security. This view of risk enables Approval Authorities to make informed decisions.

- Design and operate ***Information Assurance within the enterprise operational environments***, as a coherent whole across the IC and DoD, enabling IA situational awareness and command and control.

- Institute a ***common process*** for the IC and DoD incorporating security engineering within "lifecycle" processes. This eliminates current security-specific processes by incorporating security processes within development and system acceptance. The common process will be adaptable to various development environments. Coupled with an ongoing validation process based on strict configuration management, continuous risk assessment, continuous monitoring, and periodic and/or ad-hoc audits this change eliminates the need for "re-accreditation" as a paperwork exercise. This process reduces the existing redundant C&A activities, unnecessary documentation, and shortens the overall process of approving systems.

The new C&A processes will ensure system certifications and accreditations accomplished by one agency are valid for all agencies. Over the next several months, quick-turnaround teams will identify and develop solutions based on these seven transformation goals.

# # #

Media with questions or interview requests can contact Maj Patrick Ryder, OSD Public Affairs, at 703-695-0195; or Mr. Ross Feinstein, ODNI Public Affairs, at 202-201-1111.