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

NEWS RELEASE

FOR IMMEDIATE RELEASE
Sept. 30, 2008

ODNI News Release No. 15-08

ODNI Announces New Security Policy for IC's Information Systems

A groundbreaking new policy from the Office of the Director of National Intelligence changes how the intelligence community and, by influence, the entire federal government will build, validate and approve information technology systems. The policy requires common security controls and risk-management procedures – a unified approach to enhance collaboration.

Intelligence Community Directive 503 covers a lot of ground, but two key details stand out: There will be a single certification and accreditation process, which means all systems must follow the same authorized security requirements. Systems managers, the policy adds, should accept security risks when necessary to yield a decision advantage from timely and accurate intelligence.

Those measures will make it easier for the IC to adopt cutting-edge technology. They also foster reciprocity as well as information sharing. If one IC element certifies a system or major application, then others in the community can trust that it is secure without spending more time and money to duplicate tests.

Director of National Intelligence Mike McConnell signed the directive on Sept. 15. It cancels and replaces Director of Central Intelligence Directive 6/3 and an accompanying implementation manual, which governed the management of intelligence information systems for the past nine years.

ODNI officials said the new policy transforms the way that secure systems will be brought on line, so that greater trust will be sown across the IT enterprise. Plus, the changes will add efficiency to the entire process, they noted.

The effort, begun roughly two and a half years ago, is the outgrowth of an intense push led by the ODNI, with critical support from several IC partners – especially the federal Committee on National Security Systems, the National Institute of Standards and Technology, and the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer in the Department of Defense.

The ODNI was represented by its Office of the Associate Director of National Intelligence and Chief Information Officer.

Buy-in from the committee, NIST and DoD was invaluable, giving the policy impact beyond the intelligence community. Furthermore, the policy's status as an official standard of the Committee on National Security Systems ensures alignment of certification and accreditation processes across all federal entities.

Intelligence Community Directive 503 is available online at http://www.dni.gov/electronic_reading_room/ICD_503.pdf.

The Director of National Intelligence oversees 16 federal organizations that make up the intelligence community. The DNI also manages the implementation of the National Intelligence Program. Additionally, the DNI serves as the principal adviser to the president, the National Security Council and the Homeland Security Council on intelligence issues related to national security.

###