



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 17 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Operations Security (OPSEC) in the Department of Defense (DoD)

On March 6, 2006, I reissued the DoD directive on OPSEC, DoD Directive 5205.02. This updated policy will assist you in your continued efforts to achieve the Department's objectives to make OPSEC a priority and to integrate OPSEC into training and awareness programs. All personnel, including force protection and operations planners, need to recognize the risks associated with compromising critical information and the countermeasures needed to mitigate those risks, and should continually assess and apply appropriate OPSEC practices to their daily missions.

The new directive requires an annual review and validation of Component OPSEC programs to be reported to the Under Secretary of Defense (Intelligence) (USD(I)). The first report is due to the office of the USD(I) by September 30, 2006. The USD(I) will provide further guidance on the content of the report.

While we have made progress the last three years, there is still much work to be done to ensure that OPSEC policies and procedures are effective. At a minimum, we need to:

- Accelerate development of the OPSEC Support Elements (OSEs) within the DoD components. These organizations will be invaluable to the revitalization of OPSEC within the Department and will be an essential resource in providing training, program development and assessment support to meet all of DoD's requirements.



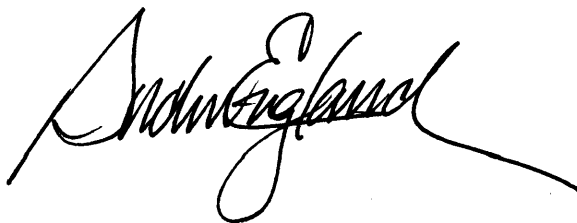
5/15/2006 2:49:02 PM

- Integrate OPSEC in innovative and practical ways as a core capability of Information Operations (IO). It is essential that sound OPSEC practices be implemented to improve the overall security of an organization. OPSEC must be executed on the battlefield and in operations planning, and must be fundamental to all DoD personnel participating in, or supporting, operations.
- Ensure OPSEC complements security practices to ensure essential protection of programs, plans, and operations. To achieve complete protection of DoD classified and unclassified but critical information, we must ensure all personnel are fully aware of their organization's OPSEC program and proscribed behaviors.
- Train DoD personnel at every level of professional development to understand intelligence threats to DoD information and to develop good OPSEC decision-making skills. We must integrate basic OPSEC principles into all military education from basic training to the most senior leadership courses. It is imperative that OPSEC be considered a priority in the classroom so that our troops are best prepared to deal with the challenges of the battlefield.

The requirement for OPSEC revitalization in the Department has not diminished. Indeed, the need for OPSEC to be integrated into all of our missions, programs and activities is magnified in overseas operations, as well as the implementation of BRAC decisions, and ever increasing challenges to protect our forces from terrorism and other threats at home and abroad. For example, current events have highlighted the need for increased attention to ensuring unclassified information posted on publicly accessible websites does not provide an adversary with information that increases the risk to our forces and infrastructure.

I applaud your contributions to OPSEC and am encouraged that we will continue to grow and invigorate the DoD OPSEC Program. The Interagency OPSEC Support Staff, (443) 479-4677, continues to be a resource to all levels of DoD. Their web site is <http://www.iooss.gov/>.

OPSEC is the responsibility of each individual in this Department. Your leadership will emphasize and enhance the protections provided to DoD operations and personnel. To deny our adversaries the opportunity to gather information on our plans, operations, and programs remains a core mission of this Department.

A handwritten signature in black ink, appearing to read "Andrew England". The signature is fluid and cursive, with a long horizontal stroke extending to the right.