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

18 OCT 2001

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
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, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR OF THE DOD FIELD ACTIVITIES

SUBJECT: Operations Security Throughout the Department of Defense

On 14 September the President declared a national emergency by reason of terrorist attacks and the continuing and immediate threat of further attacks on the United States. As this Department assists wide-ranging efforts to defeat international terrorism, it is clear that US military and civilian service lives, DOD operational capabilities, facilities and resources, and the security of information critical to the national security will remain at risk for an indefinite period.

It is therefore vital that Defense Department employees, as well as persons in other organizations that support DOD, exercise *great* caution in discussing information related to DOD work, regardless of their duties. Do not conduct *any* work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits. Classified information may be discussed *only* in authorized spaces and with persons having a specific need to know and the proper security clearance. Unclassified information may likewise require protection because it can often be compiled to reveal sensitive conclusions. Much of the information we use to conduct DOD's operations must be withheld from public release because of its sensitivity. If in doubt, do not release or discuss official information except with other DoD personnel.

All major components in this Department to include the Office of the Secretary of Defense, the Military Departments, the Joint Staff, the Combatant Commands, the Defense Agencies, the DOD Field Activities and all other organizational entities within the DOD will review the Operations Security (OPSEC) Program, described in DOD Directive 5205.2, and ensure that their policies, procedures and personnel are in compliance. We must ensure that we deny our adversaries the information essential for them to plan, prepare or conduct further terrorist or related hostile operations against the United States and this Department.

Paul Wolfowitz