



ACQUISITION  
TECHNOLOGY  
AND LOGISTICS

OFFICE OF THE UNDER SECRETARY OF DEFENSE  
3000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

SEP 8 2008

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY  
(ACQUISITION, LOGISTICS & TECHNOLOGY)  
ASSISTANT SECRETARY OF THE NAVY  
(RESEARCH, DEVELOPMENT & ACQUISITION)  
ASSISTANT SECRETARY OF THE AIR FORCE  
(ACQUISITION)  
DIRECTORS OF DEFENSE AGENCIES  
DIRECTORS OF DEFENSE FIELD ACTIVITIES

SUBJECT: Control of Information Technology Property Containing Sensitive  
Information

The Department of Defense Inspector General (DoDIG) report: "Audit of Controls and Accountability of Defense Security Service Assets Containing Personal Records or Classified Information" (Report D-2008-114) revealed potential control weaknesses involving information technology (IT) property containing personally identifiable information (PII). Such data is or can be linked to an individual person, e.g., name, social security number, date and place of birth, mother's maiden name, biometric records, etc.

Any IT property containing PII [or Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI)] must be controlled and managed in a manner that protects against the unauthorized use, disclosure, or loss of such information. The DoDIG recommended that DoD policy be updated to reflect this requirement.

Accordingly, this requirement will be highlighted in the next update of DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property." In the interim, please ensure that IT property, e.g., desktops, laptops, and mobile computing devices, containing PII [or SBU or CUI] is properly accounted for and controlled, and that appropriate safeguards are in place to prevent unauthorized use, disclosure or loss of sensitive information.

Questions concerning this memorandum should be directed to Ms. Sarah Ball at 703-604-6350 x 103.

Nancy L. Spruill

Director, Acquisition Resources & Analysis

