



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

APR 18 2006

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Protection of Sensitive Department of Defense (DoD) Data at Rest
On Portable Computing Devices

The proliferation of portable computing devices across the DoD requires a fresh look at current policies governing the protection of sensitive data at rest. Recent advances in computing technology have resulted in greatly increased computing power and storage capacity for portable computing devices. These advances have enhanced both effectiveness and efficiency by allowing DoD personnel to perform their duties at home or while on official travel, but they are not without costs. Along with the increased computing capability and portability there are also more and greater threats to the unclassified sensitive DoD information that is likely to be resident on the hard drives of the devices. Portable computing devices are much more likely to be lost, stolen, or exploited while unattended than are those that permanently remain in office spaces.

This memorandum provides suggestions on technical means to protect unclassified sensitive information on portable computing devices used within DoD. The measures are in addition to the normal physical security required for such devices so that, if they fall into the wrong hands for any reason, access to the sensitive DoD information they



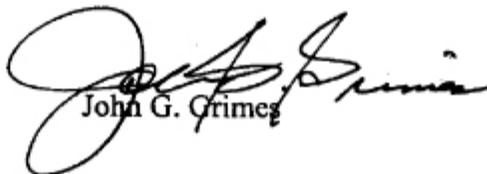
contain will be much more difficult. Most of these measures are relatively inexpensive and can be implemented in a short period of time. They include:

- Encryption of only the resident information on the hard drives of portable computing devices where encryption technology is available for the device in question.
- Identity and authentication controls to manage access to the device. Such controls should be consistent with DoD PKI policies to the extent possible.
- Passwords to control access to encrypted, as well as unencrypted, material.

Components are also reminded that IA and IA-enabled products are required to comply with the evaluation and validation requirements detailed in paragraph E3.2.5. of DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

While the protective measures described above are in the form of suggestions, most are expected to become policy requirements in the not-too-distant future and all DoD Components are strongly encouraged to adopt them as soon as possible. Priority should be given to protecting information on portable computing devices used by senior officials and other individuals who travel frequently, particularly to areas where loss or exploitation of the devices is more likely or when the consequence of the loss would be more severe.

Information on encryption products and other implementation details may be found at <http://iase.disa.mil>. The DoD CIO point of contact for this initiative is [REDACTED] of the Defense-wide Information Assurance Program Office at (703) 604-0503 [REDACTED].


John G. Grimes

cc:
Chief Information Officers of the DoD Components