DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 17 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, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Computer Forensic Laboratory (DCFL), and Department of Defense Computer Investigations Training Program (DCITP)

This policy letter defines the mission, organizational structure, resources, and services provided by the DCFL and DCITP.

- The DCFL's mission is to provide digital evidence processing and analysis for DoD, set DoD guidelines for digital forensic analysis, foster forensic media analysis RDT&E projects, and conduct liaison by partnering with governmental and private industry computer security officials to keep abreast of cutting edge technology.
- The DCITP's mission is to provide computer investigations training to forensic examiners, investigators, system administrators, or any other DoD member who helps ensure Defense information systems are secure from unauthorized use.

The Secretary of the Air Force serves as the DoD Executive Agent for these activities, and the Commander of the Air Force Office of Special Investigations (AFOSI) provides overall program management.

All Defense Chief Information Officers and the Joint Task Force Computer Network Operations, should integrate these services and information into their business processes to help safeguard their systems. A list of implementing guidelines is attached.

This policy is effective immediately and will be codified in the DoD Directive System.

Paul Wolfowitz

Attachment

U13620 /01

Implementing Guidelines for DCFL and DCITP

Consistent with the direction set out in Department of Defense (DoD) Reform Initiative #27, dated February 10, 1998, the DCFL and DCITP are fully operational. The DCFL is also authorized to support any DoD investigation (to include safety investigations, Inspector General directed inquiries, and commander inquiries) that requires computer forensic support to detect, enhance, or recover digital media, to include audio and video. The DCFL and DCITP should integrate their activities to support infrastructure protection and information operations for on-going programs and initiatives including the Critical Infrastructure Protection (CIP) program. They should also be actively engaged in related exercises. Both the training and forensic programs will continue to seek accreditation and appropriate certifications.

Funding of these programs was realigned to the Air Force in FY2000. Previous cost sharing was conducted by 12 Defense Agencies under separate Memoranda of Agreement (MOA). Business enterprise and fee for service is authorized in accordance with (IAW) the Economy Act, and all services to non-DoD organizations will be provided IAW the Economy Act or other applicable authority. To the extent that DCFL and DCITP resources are insufficient to meet requirements of DoD organizations that may result in extensive TDYs or expanding existing training, DoD organizations may be required to fund that effort or provide reimbursement IAW the financial management regulations. All agencies, both DoD and non-DoD, are encouraged to establish a MOA with DCFL and DCITP before they seek DCFL's and DCITP's assistance. Each MOA should specifically address personnel, facilities, reimbursement, and authority.

Once a MOA is signed, a forensic request can be submitted using guidance found at www.dcfl.gov. All forensic support requests will be assigned a category (I, II, III, IV, or V) which reflects the priority of the case based on national security implications. An internal DCFL management system will track chain of custody and the status of each matter.

For training information, agencies should contact registrar@dcitp.gov or visit their web site at www.dcitp.gov. Training will be based on an annual assessment that allocates a quota percentage of available training. Any quota not filled will be offered to the first named alternate submitted by any Service or Defense Agency following notice of the vacancy. All requests from civilian (non-DoD) agencies for forensic laboratory or training support will be handled on a case-by-case basis consistent DoD Directive 5525.5 *DoD Cooperation with Civilian Law Enforcement Officials*. This supports PDD-63, CIP direction for a public-private partnership to reduce critical infrastructure vulnerabilities. Requests should be submitted to DCFL or DCITP to be forwarded as necessary, through the AFOSI Commander, to the Secretary of the Air Force Inspector General's Special Investigations Directorate (SAF/IGX) for a decision by Secretary of the Air Force or his/her designee.