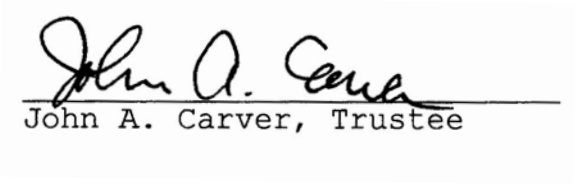
MANAGEMENT AND ADMINISTRATION DIRECTIVE 500.2

SUBJECT: Safeguarding Sensitive, Unclassified Information

EFFECTIVE DATE: May 5, 2000

APPROVED: 
John A. Carver, Trustee

I. INTRODUCTION: The Court Services and Offender Supervision Agency and the Pretrial Services Agency (hereinafter referred to collectively as "Agency") both play a critical role in law enforcement and public safety in the District of Columbia. As a result, most employees of the Agency are processing, handling, or working with sensitive, unclassified information (e.g., Privacy Act Protected, alcohol and drug treatment records, fiduciary, investigative, law enforcement, medical, offender, personnel, etc.). This information, regardless of format (i.e., files, records, computer data, etc.) must be safeguarded against unauthorized disclosure, modification, access, use, or destruction.

II. PURPOSE: The purpose of this Directive is to outline the Agency policy for safeguarding sensitive, unclassified information.

III. COVERAGE: This Directive applies to all personnel employed by the Agency, to include contractors and consultants.

IV. DEFINITIONS:

Classified Information – Any information that has been determined, pursuant to Executive Order (E.O.) 12958, Classified National Security Information, to require protection against unauthorized disclosure and is marked (i.e., Top Secret, Secret, or Confidential) to indicate its classified status. ***It should be noted that the Agency does not normally receive, produce,***

process, or store classified information. Should anyone receive this type of information, contact the Office of Security.

Sensitive, Unclassified Information – Any information, the loss, misuse, modification of or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an E.O. or an act of Congress to be kept classified in the interest of national defense or foreign policy.

V. POLICY:

A. Sensitive, unclassified information includes, but is not limited to Privacy Act Protected, fiduciary, investigative, law enforcement, medical, offender, personnel, or other information which, the unauthorized disclosure of could result in harm or unfair treatment to any individual or group, or have a negative impact upon the Agency. In addition, this policy implements the safeguarding requirements of 42 C.F.R., Section 2.16, Confidentiality of Alcohol and Drug Treatment Records.

B. Agency employees have the responsibility for safeguarding, to an appropriate degree, the sensitive, unclassified information that they process or handle.

C. Individuals employed by the Agency shall take reasonable steps to protect sensitive, unclassified information in their custody from unauthorized access, modification, destruction, or disclosure. Employees who are uncertain about the appropriate degree of protection to afford the sensitive, unclassified information are required to request guidance from the Agency's Freedom of Information Act (FOIA) Officer.

D. Supervisors are responsible to ensure that a copy of this policy is provided to each of their employees.

VI. PROTECTIVE MEASURES:

A. DISSEMINATION and METHODS OF TRANSMISSION. Employees must consider the sensitivity of requested information and the recipient's need-to-know before they disseminate or authorize the dissemination of sensitive, unclassified information. The requested information, if authorized for release, may be transmitted via inter-office mail, e-mail, or similar channels;

however, on occasion, the nature of the requested information or the lack of control over intermediate recipients may warrant greater protection, such as personal delivery. Requested information, if authorized for release, may also be sent via the U.S. Postal Service or commercial courier, provided it is packaged in a way that does not disclose its contents or the fact that is it sensitive, unclassified information. Employees who are uncertain about the dissemination or an appropriate method of transmission are required to request assistance from the Agency's FOIA Officer.

B. STORAGE. Sensitive, unclassified information shall be stored in ways that do not expose the Agency to undue risk or harm from the unauthorized access, modification, destruction, or disclosure. In offices or areas with access control devices (i.e., electronic security, cipher locks, key locks, etc.) it may be acceptable to store the information on or in desks, or file cabinets. However, in offices or areas without access control devices, employees will have to take greater precautions, such as storing the material in a locked desk, file cabinet or security container. Each employee will ensure that the following security measures are taken:

1. When sensitive, unclassified information is not under the control of an authorized person, the information will be stored in a manner prescribed above.

2. At the end of each business day, all sensitive, unclassified information will be stored in a manner prescribed above.

C. COMPUTER TECHNOLOGY. The Chief Technology Officer is responsible for the development and implementation of access control policies and procedures to ensure that protective measures are provided for the Agency telecommunications and automated information and systems which process sensitive, unclassified information. In addition, employees are responsible for complying with the Information Technology policies and procedures that govern user requirements for safeguarding sensitive, unclassified information.

D. DISPOSAL. Pursuant to Title 44 of the United States Code, Public Printing and Documents, as supplemented by Agency policy, each Program Manager must establish records management procedures for the records maintained in their respective organization. When the disposal of sensitive, unclassified

information is required, it must be accomplished by shredding or burning.