

12 FAM 540

SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU)

(TL:DS-61; 10-01-1999)

12 FAM 541 SCOPE

(TL:DS-46; 05-26-1995)

a. SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act.

b. SBU information includes, but is not limited to:

(1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and

(2) Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers.

12 FAM 542 IMPLEMENTATION

(TL:DS-46; 05-26-1995)

Previous regulations regarding LOU material are superseded and LOU becomes SBU as of the date of this publication.

12 FAM 543 ACCESS, DISSEMINATION, AND RELEASE

(TL:DS-61; 10-01-1999)

a. U.S. citizen direct-hire supervisory employees are responsible for access, dissemination, and release of SBU material. Employees will limit access to protect SBU information from unintended public disclosure.

b. Employees may circulate SBU material to others, including Foreign Service nationals, to carry out an official U.S. Government function if not otherwise prohibited by law, regulation, or interagency agreement.

c. SBU information is not required to be marked, but should carry a distribution restriction to make the recipient aware of specific controls. To protect SBU information stored or processed on automated information systems, the requirements found in 12 FAM 600 (Information Security Technology) must be met.

12 FAM 544 SBU HANDLING PROCEDURES: TRANSMISSION, MAILING, SAFEGUARDING/STORAGE, AND DESTRUCTION

(TL:DS-47; 06-08-1995)

a. Regardless of method, transmission of SBU information should be effected through means that limit the potential for unauthorized public disclosure. Since information transmitted over unencrypted electronic links such as telephones may be intercepted by unintended recipients, custodians of SBU information should decide whether specific information warrants a higher level of protection accorded by a secure fax, phone, or other encrypted means of communication.

b. SBU information may be sent via the U.S. Postal Service, APO, commercial messenger, or unclassified registered pouch, provided it is packaged in a way that does not disclose its contents or the fact that it is SBU.

c. During nonduty hours, SBU information must be secured within a locked office or suite, or secured in a locked container.

d. Destroy SBU documents by shredding or burning, or by other methods consistent with law or regulation.

12 FAM 545 RESPONSIBILITIES

(TL:DS-46; 05-26-1995)

Unauthorized disclosure of SBU information may result in criminal and/or civil penalties. Supervisors may take disciplinary action, as appropriate. State offices responsible for the protection of records are outlined in 5 FAM. See 3 FAM for regulations and process on disciplinary actions. (12 FAM 550 provisions regarding incidents/violations do not pertain to SBU.)

12 FAM 546 THROUGH 549 UNASSIGNED