

SENSITIVE BUT UNCLASSIFIED

In accordance with 12 FAM 540 (see reverse), Sensitive but Unclassified material should be handled and transmitted through means which will limit the potential for unauthorized public disclosure. It must be secured within a locked office or suite, or a locked container during non-duty hours.

(This cover sheet is unclassified)

SENSITIVE BUT UNCLASSIFIED

12 FAM 540

SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU)

(CT:DS-190; 03-05-2013)

(Office of Origin: DS/SI/IS)

- **12 FAM 541 SCOPE** (CT:DS-190; 03-05-2013) a. Sensitive but unclassified (SBU) information is information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons. SBU should meet one or more of the criteria for exemption from public disclosure under the Freedom of Information Act (FOIA) (which also exempts information protected under other statutes), 5 U.S.C. 552, or should be protected by the Privacy Act, 5 U.S.C. 552a. b. Types of unclassified information to which SBU is typically applied include all FOIA exempt categories (ref. **5 U.S.C. 552b**), (examples are listed in 12 FAM 541. c. Designation of information as SBU is important to indicate that the information requires a degree of protection and administrative control but the SBU label does not by itself exempt information from disclosure under the FOIA (5 U.S.C. 552b). Rather, exemption is determined based on the nature of the information in question.
- **12 FAM 543 ACCESS, DISSEMINATION, AND RELEASE** (CT:DS-161; 03-01-2011) a. U.S. citizen direct-hire supervisory employees are ultimately responsible for access, dissemination, and release of SBU material. All employees will limit access to protect SBU information from unauthorized or unintended disclosure. b. In general, employees may circulate SBU material within the Executive Branch, including to locally employed staff (LE staff), where necessary to carry out official U.S. Government functions. However, additional restrictions may apply to particular types of SBU information by virtue of specific laws, regulations, or international or interagency agreements. Information protected under the Privacy Act, can only be distributed within the Department of State on a “need-to-know” basis and cannot be distributed outside the Department of State except as permitted by specific statutory exemptions or “routine uses” established by the Department of State. c. Before distributing any SBU information, employees must be sure that such distribution is permissible and, when required, specifically authorized. (See [5 FAM 470](#).) d. SBU information must be marked whenever practical to make the recipient aware of specific controls. While some documentation, such as standard forms and medical records, does not lend itself to marking, many documents, such as emails, cables, and memoranda, can, and must be marked in accordance with [5 FAM 751.3](#), 5 FAH 1 H-200 and 5 FAH-1 H 135. e. SBU information that is not to be released to non-U.S. citizens, including locally employed staff, must be marked SBU/NOFORN (Not for release to foreign nationals (NOFORN)). The specific requirements for SBU/NOFORN are identified in [12 FAM 545](#). f. Information obtained from or exchanged with a foreign government or international organization as to which public release would violate conditions of confidentiality or otherwise harm foreign relations must be classified in order to be exempt from release under FOIA or other access laws. The SBU label cannot be used instead of classification to protect such information. g. Where an individual has expressly authorized his or her personal information to be sent unencrypted over any unsecured electronic medium, such as the Internet, fax transmission, or wireless phone, such information may be transmitted without regard to the provisions and policies set forth in this subchapter. See 5 FAH-4, H-442 for guidance on obtaining an individual’s authorization to transmit personal information in this manner.
- **12 FAM 544 SBU HANDLING PROCEDURES** (CT:DS-117; 11-04-2005) a. Regardless of method, the handling, processing, transmission and/or storage of SBU information should be effected through means that limit the potential for unauthorized disclosure. b. Employees while in travel status or on temporary duty (TDY) assignment should ensure that SBU is adequately safeguarded from unauthorized access in light of the threat conditions and nature of the SBU (see [12 FAM 544.1](#) d.) (This applies regardless of whether the information is being transported in paper form, CDs, diskettes and other electronic readable media, or on a portable digital device; such as a laptop, wireless or wired, or PDA.)

Additional SBU guidance is contained within 12 FAM 540