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)**, for example:

(1) Personnel, payroll, medical, passport, adoption, and other personal information about individuals, including social security numbers and home addresses and including information about employees as well as members of the public;

(2) Confidential business information, trade secrets, contractor bid or proposal information, and source selection information;

(3) Department records pertaining to the issuance or refusal of visas, other permits to enter the United States, and requests for asylum;

(4) Law enforcement information or information regarding ongoing investigations;

(5) Information illustrating or disclosing infrastructure protection vulnerabilities, or threats against persons, systems, operations, or facilities (such as, usernames, passwords, physical, technical or network specifics, and in certain instances, travel itineraries, meeting schedules or attendees), but not meeting the criteria for classification under *Executive Order (EO) 13526, dated December 29, 2009*;

(6) Information not customarily in the public domain and related to the protection of critical infrastructure assets, operations, or resources, whether physical or cyber, as defined in the Homeland Security Act, 6

U.S.C. 131(c);

(7) Design and construction information;

(a) Certain information relating to the design and construction of diplomatic missions abroad, such as graphic depictions of floor plans and specifications for foreign affairs offices and representational housing overseas, as outlined in the DS Security Classification Guide for the Design and Construction of Overseas Facilities, dated May 2003; and

(b) Certain information relating to the design and construction drawings and specifications of General Service Administration (GSA) facilities, as outlined in GSA Order PBS *3490.1A, dated June 1, 2009*.

(8) Privileged attorney-client communications (relating to the provision of legal advice) and documents constituting attorney work product (created in reasonable anticipation of litigation); and

(9) Inter or intra-agency communications, including emails, that form part of the internal deliberative processes of the U.S. Government, the disclosure of which could harm such processes.

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 542 IMPLEMENTATION

(CT:DS-117; 11-04-2005)

This policy is effective 11-04-2005.

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.)

12 FAM 544.1 Fax Transmission, Mailing, Safeguarding/Storage, and Destruction of SBU

(CT:DS-117; 11-04-2005)

a. Unintended recipients can intercept SBU information transmitted over unencrypted electronic point-to-point links, such as Voice over Internet Protocol methodology (VoIP), telephones or faxes.

b. Employees transmitting SBU information should consider whether specific information warrants a higher level of protection accorded by a secure fax, phone, or other encrypted means of communication. Employees transmitting SBU information via non-secure fax must ensure that an authorized recipient is ready to receive it at the other end.

c. SBU information may be sent via the U.S. Postal Service (USPS) or a commercial delivery service, e.g., Fed Ex, DHL. SBU information, except SBU/NOFORN, (see 12 FAM 545) mailed to posts abroad should be sent via unclassified registered pouch or to a Military Postal Facility (MPF) via USPS, whenever practicable. Use of foreign mail services is authorized, if required. Except in those cases where the pouch is utilized, mail must be packaged in a way that does not disclose its contents or the fact that it is SBU.

d. During non-duty hours, SBU information and removable electronic media in U.S. Government facilities must be secured within a locked office or suite, or secured in a locked container. Employees in possession of SBU outside U.S. Government facilities must take adequate precautions that afford positive accountability of the information and to protect SBU information from unauthorized access such as storage in a locked briefcase or desk in a home office. SBU should not be left unsecured (e.g. lock in room safe) in unoccupied hotel rooms or unattended in other public spaces.

e. Custodians of medically privileged information must ensure that it is secured when not in use.

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

12 FAM 544.2 Automated Information System (AIS) Processing and Transmission

(CT:DS-117; 11-04-2005)

The requirements for processing SBU information on a Department AIS are established in 12 FAM 620 and 5 FAM 700. Where warranted by the nature of the information, employees who will be transmitting SBU information outside of the Department network on a regular basis to the same official and/or most personal addresses, should contact IRM/OPS/ITI/SI/PKI to request assistance in providing a secure technical solution for those transmissions. Availability of a Public Key

Infrastructure (PKI) solution for a home computer will depend upon the computer's operating system (e.g., Windows(r) XP). Employees participating in the home PKI and telework program must complete the requisite training and sign an acknowledgement statement prior to being issued the approved security measures/equipment.

12 FAM 544.3 Electronic Transmission Via the Internet

(CT:DS-117; 11-04-2005)

a. It is the Department's general policy that normal day-to-day operations be conducted on an authorized AIS, which has the proper level of security control to provide nonrepudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information. The Department's authorized telework solution(s) are designed in a manner that meet these requirements and are not considered end points outside of the Department's management control.

b. The Department is expected to provide, and employees are expected to use, approved secure methods to transmit SBU information when available and practical.

c. Employees should be aware that transmissions from the Department's OpenNet to and from non-U.S. Government Internet addresses, and other .gov or .mil addresses, unless specifically directed through an approved secure means, traverse the Internet unencrypted. Therefore, employees must be cognizant of the sensitivity of the information and mandated security controls, and evaluate the possible security risks and then decide whether a more secure means of transmission is warranted (i.e., secure fax, mail or network, etc.)

d. In the absence of a Department-provided secure method, employees with a valid business need may transmit SBU information over the Internet unencrypted after carefully considering that:

(1) SBU information within the category in 12 FAM 541b(7)(a) and (b) must never be sent unencrypted via the Internet;

(2) Unencrypted information transmitted via the Internet is susceptible to access by unauthorized personnel;

(3) Email transmissions via the Internet generally consist of multipoint communications that are routed to their destination through the path of least resistance, which may include multiple foreign and U.S. controlled Internet service providers (ISP);

(4) Once resident on an ISP server, the SBU information remains until it is overwritten;

(5) Unencrypted email transmissions are subject to a risk of compromise of information confidentiality or integrity;

(6) SBU information resident on personally owned computers connected to the Internet is generally more susceptible to cyber attacks and/or compromise than information on government owned computers connected to the Internet;

(7) The Internet is globally accessed (i.e., there are no physical or traditional territorial boundaries). Transmissions through foreign ISPs or servers can magnify these risks; and

(8) Current technology can target specific email addresses or suffixes and content of unencrypted messages.

e. SBU information must not be posted on any public Internet website, discussed in a publicly available chat room or any other public forum on the Internet.

f. To preclude inadvertent transmission of SBU information prohibited on the Internet, AIS users must not use an "auto-forward" function to send emails to an address outside the Department's network.

g. SBU information created on or downloaded to publicly available non- U.S. Government owned computers, such as Internet kiosks, should be removed when no longer needed.

h. All users who process SBU information on personally owned computers must ensure that these computers will provide adequate and appropriate security for that information. This includes:

(1) Disabling unencrypted wireless access;

(2) The maintenance of adequate physical security;

(3) The use of anti-virus and spyware software; and

(4) Ensuring that all operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions are current.

12 FAM 544.4 SBU Transmission Between State Department Facilities

(CT:DS-117; 11-04-2005)

All SBU transmissions between Department facilities must be encrypted to current NIST, DS, and IT CCB standards.

12 FAM 545 SBU/NOFORN INFORMATION

(CT:DS-117; 11-04-2005)

a. SBU/NOFORN information is information determined by the originator or a classification guide to be prohibited for dissemination to non-U.S. citizens. It must be labeled SBU/NOFORN.

b. As the NOFORN caveat indicates, this type of SBU information warrants a degree of protection greater than that of standard SBU information. Therefore, employees must:

(1) Process and transmit SBU/NOFORN information only on a system authorized by the Department for classified information transmission, storage and processing;

(2) Fax or discuss (over telephone lines) SBU/NOFORN information only via encrypted telephone lines;

(3) Mail SBU/NOFORN information to posts via classified pouch or to a MPF via USPS registered mail. Mail sent via USPS registered must be packaged in a way that does not disclose its contents or the fact that it is SBU/NOFORN;

(4) Secure SBU/NOFORN information during non-duty hours following the same guidelines for CONFIDENTIAL information; and

(5) Destroy SBU/NOFORN documents in a Department-approved manner, such as by shredding, burning, or other methods consistent with law or regulation for the destruction of classified information.

12 FAM 546 THROUGH 549 UNASSIGNED