

United States Department of State

Office of the Director of U.S. Foreign Assistance (F)

**Foreign Assistance Coordination and Tracking System (FACTS)
and FACTS Info**

Data Use Policy

June 11, 2009

Submitted by
Program Management Office (F/PM)

TABLE OF CONTENTS

1. INTRODUCTION.....	1
2. DATA SENSITIVITY	1
3. DATA IDENTIFICATION	1
3.1 SOURCE	1
3.2 SENSITIVITY MARKINGS.....	2
4. DATA FOR INTERNAL USG USE	2
5. DATA FOR EXTERNAL USE	2
6. CLEARANCE PROCESS.....	3

LIST OF ANNEXES

Annex 1	TABLE SUMMARIZING F DATA POLICY	A1-1
Annex 2	12 FAM 540	A2-1
	12 FAM 541 SCOPE	A2-1
	12 FAM 542 IMPLEMENTATION	A2-2
	12 FAM 543 ACCESS, DISSEMINATION, AND RELEASE	A2-2
	12 FAM 544 SBU HANDLING PROCEDURES	A2-3
	12 FAM 544.1 FAX TRANSMISSION, MAILING, SAFEGUARDING/STORAGE, AND DESTRUCTION OF SBU	A2-4
	12 FAM 544.2 AUTOMATED INFORMATION SYSTEM (AIS) PROCESSING AND TRANSMISSION	A2-5
	12 FAM 544.3 ELECTRONIC TRANSMISSION VIA THE INTERNET	A2-5
	12 FAM 544.4 SBU TRANSMISSION BETWEEN STATE DEPARTMENT FACILITIES	A2-7
	12 FAM 545 SBU/NOFORN INFORMATION.....	A2-7

1. INTRODUCTION

This document is a guide to using and sharing data contained in the Foreign Assistance Coordination and Tracking System (FACTS) and FACTS Info. This policy applies to all FACTS and FACTS Info users and to all data contained within the system without exception.

2. DATA SENSITIVITY

FACTS and FACTS Info contain Sensitive But Unclassified (SBU) and unclassified data. The SBU information included in FACTS and FACTS Info, and communications stemming from or in support of those systems, involve the following sensitivities (See Annex 2: 12 FAM 540):

1. Confidential business information, trade secrets, contractor bid or proposal information and source selection information;
2. Inter/Intra-agency communications, including e-mail messages, that form part of the internal deliberative processes of the US Government, the disclosure of which could harm such processes.

This document outlines (1) the types of information that are considered SBU and are therefore subject to restrictions and (2) data that can be shared without additional clearance.

3. DATA IDENTIFICATION

All FACTS/FACTS Info users are responsible for ensuring that reports and documents generated from FACTS/FACTS Info are clearly labeled with the appropriate source and sensitivity markings as described below.

3.1 SOURCE

Reports and documents generated from FACTS/FACTS Info must be labeled with the following source information. These labels will be automatically generated for all reports run from FACTS Info. Users must ensure that these labels are retained in the reports and/or added to relevant documents when sharing them with others:

- 1.) The Office of the Director of U.S. Foreign Assistance;
- 2.) The data category: e.g., Central Budget, Performance Report, Operational Plan, Mission Strategic Plan, etc. (see Category column in the reference table on pp. A1-1-A1-2);
- 3.) The data column header: e.g., 200X Actual Base, 200X OMB Narratives, etc. (see Data column in the reference table on pp. A1-1-A1-2);
- 4.) The Operating Unit; and
- 5.) The date the report was generated.

For Example:

1. Office of the Director of US Foreign Assistance, Central Budget; 200X Actual Base, Zambia; January X, 200X.

In addition, if data obtained from FACTS or FACTS Info originated from an external source (e.g., World Bank or UNAIDS HIV/AIDS data included in Operational Plan narratives), the FACTS/FACTS Info user is required to cite the original data source when sharing this information.

3.2 SENSITIVITY MARKINGS

FACTS/FACTS Info users must clearly label all reports and documents with all applicable sensitivity and/or classification levels. For example, if a report/document is SBU (see Section 4), it must be marked accordingly and documents restricted to USG audiences must be marked “USG Only – Not for Distribution.” Draft documents should include the draft watermark or a “draft” header on every page of the document.

4. DATA FOR INTERNAL USG USE

Much of the data included in FACTS and FACTS Info is restricted to internal USG use, which restricts dissemination to USG direct hire personnel, and individuals who are performing official governmental functions on behalf of the USG, such as contractors and locally employed staff, as appropriate and necessary. However, not all data can be shared with all USG audiences, and much of the data in FACTS and FACTS Info cannot be shared outside the Department of State and USAID without special authorization. The table in Annex I summarizes the data available in FACTS and FACTS Info and the restrictions applicable to the various types of information.

There are certain restrictions on data for internal USG use. All documents produced using FACTS or FACTS Info data must be labeled appropriately as described in Sections 2 and 3 of this document and circulated, filed, stored or discarded/destroyed in accordance with USG requirements. Please refer to Annex 2 for guidance on procedures pertaining to SBU information.

SBU Data: Financial data from the current fiscal year Operational Plan is considered to be procurement-sensitive and SBU and must be treated as outlined in Annex 2. It should only be shared as necessary and allowable and is restricted to State/USAID use. The following types of data fall into this category:

1. Organization Type 1
2. Organization Type 2
3. Partner Name
4. Budget Information Related to Partners
5. Mechanism Type
6. USG Agency
7. Mechanism Name
8. Benefiting XXX Bureau
9. Benefiting Country
10. 200X Op Plan - Initial

In addition, pre-decisional budget data is considered SBU and subject to various restrictions. Please refer to Annex 1 to determine which types of data can be shared with which audiences.

5. DATA FOR EXTERNAL USE

Data listed as Public in Annex 1 may be shared with other USG agencies and outside the USG. Data is considered public after it has been released by F. Additional restrictions applicable to implementing partners are described below. Please refer to the Clearance Procedures described in Section 6 that are applicable in certain circumstances.

Budget Data: F maintains a report(s) on their websites (<http://inside.usaid.gov/AF/index.html> and <http://www.state.gov/f/>) that provide publicly available budget data from FACTS/FACTS Info in a format for use by members of the public. To ensure that information disseminated with the public is accurate, up-to-date, and complete, all requests for Public FACTS/FACTS Info budget

data should be addressed using this report(s). Raw budget data from FACTS/FACTS Info should not be shared with the public. Questions or requests regarding budget data should be addressed to FACTSInfoSupport@state.gov.

Other types of Data/Information: FACTS/FACTS Info users may share non-budgetary data from FACTS/FACTS Info that is listed as Public in Annex 1 (e.g., CBJ Request narrative and performance results and targets) without further clearance.

Implementing Partners: Only data listed as Public in Annex 1 may be shared with implementing partners. As described in Section 4, data pertaining to implementing partners in the current year Operational Plan is considered SBU and procurement-sensitive and cannot be shared outside of USAID and State.

Questions/Requests for Assistance: If FACTS/FACTS Info Users or members of the public need assistance using FACTS/FACTS Info data or the publicly available report(s), they should address their questions to FACTSInfoSupport@state.gov.

6. CLEARANCE PROCESS

The F Data Policy table included in Annex 1 of this document defines the levels of restriction that apply to various FACTS/FACTS Info data. Sections 4 and 5 of this document describe additional restrictions. All FACTS/FACTS Info users are responsible for adhering to these requirements.

The following clearance procedures must be followed prior to sharing FACTS/FACTS Info data with certain audiences. In all cases, prior to the dissemination of information from FACTS/FACTS Info, the responsible individual must ensure that it is accurate, that it reflects current Foreign Assistance policies and procedures, that it is appropriate for the situation/request, is labeled as required, and that any disclosure is authorized by law. In the case of business-proprietary information, any disclosure in a manner or to an extent not authorized by law can result in criminal penalties.

Congress and the Executive Office of the President (EOP), to include OMB: Annex 1 indicates which data can be shared with the Congress and the EOP. The following procedures must be followed before FACTS/FACTS Info data is disseminated to these audiences.

Step 1: Requests originating in USAID or State should be forwarded to the relevant USAID or State bureau Development Planner (DP) or Bureau Planner (BP). The DP or BP should develop a response by pulling the appropriate information from FACTS/FACTS Info and forward the draft response to the F Point of Contact (POC) for review and clearance.¹

Step 2: The F/POC reviews the information submitted to them by the BP/DP or originates a report/draft response if the original request was addressed to them. The F/POC reviews and clears the information ensuring that it is appropriate to share with these audiences as determined by the Annex 1 table; that it is accurate; that it reflects current Foreign Assistance policies and procedures; that it is appropriate for the situation/request; is labeled as required; and that any disclosure is authorized by law.

¹ For questions on names of current F Points of Contacts, please email F_Staff_Assistant, or call 202-647-1086.

Step 3: After the F/POC has reviewed and cleared the information, they must forward information for Congressional audiences to the F/Congressional Liaison for clearance and information for EOP audiences should be forwarded to the F/Chief of Staff for clearance. Following clearance by the F Congressional Liaison or Chief of Staff, the information may be disseminated to the requestor. For Congressional audiences, State/H or USAID/LPA will review the information before transmitting to Congress.

ANNEX 1: F DATA POLICY

This table describes the level of restrictions for sharing FACTS and FACTS Info data. Data may be shared with audiences as designated below by X. All requirements and descriptions discussed in previous sections of this document apply.

F Data Policy								
Clearance Process	Category	Data*	Data Audiences (order based on level of restriction)					
			Internal F	State USAID Washington	State USAID Field	Executive Office of the President/OMB	Congress	Public
Public Information**	Central Budget	200X Actual Base	X	X	X	X	X	X
	Central Budget	200X Actual Supp	X	X	X	X	X	X
	Central Budget	200X Actual Total	X	X	X	X	X	X
	Central Budget	200X Estimate Base	X	X	X	X	X	X
	Central Budget	200X Estimate Supp	X	X	X	X	X	X
	Central Budget	200X Estimate Total	X	X	X	X	X	X
	Central Budget	200X Request Base	X	X	X	X	X	X
	Central Budget	200X Request Supp	X	X	X	X	X	X
	Central Budget	200X Request Total	X	X	X	X	X	X
	Central Budget	Key Areas	X	X	X	X	X	X
	Central Budget	200X 653(a) Final Base	X	X	X	X	X	X
	Earmark/Account Controls	200X Earmark Controls	X	X	X	X	X	X
	Central Budget	200X CBJ Request Narratives	X	X	X	X	X	X
	Performance Report	Performance Results and Targets	X	X	X	X	X	X
	Performance Report	All Performance Narratives	X	X	X	X	X	X
Restricted Information**	Central Budget	200X OMB Narratives	X	X		X		
	Central Budget	200X Out Year Budget Formulation Narratives	X	X				
	Central Budget	200X 653(a) Initial Base	X	X		X		
	Central Budget	200X OMB Base	X	X		X		
	Mission Strategic Plan	200X MSP Constrained	X	X				
	Mission Strategic Plan	200X MSP Preferred	X	X				
	Central Budget	200X Bureau Constrained	X	X				
	Central Budget	200X Bureau Change	X	X				
	Central Budget	200X Bureau Preferred	X	X				
Central Budget	200X Bureau Constrained Final	X	X					

F Data Policy								
Clearance Process	Category	Data*	Data Audiences (order based on level of restriction)					
			Internal F	State USAID Washington	State USAID Field	Executive Office of the President/OMB	Congress	Public
Restricted Information**	Central Budget	200X Bureau Change Final	X	X				
	Central Budget	200X Bureau Preferred Final	X	X				
	Central Budget	200X F Rec. Change	X					
	Central Budget	200X F Rec. Total	X					
	Central Budget	200X Freeze	X	X				
	Central Budget	200X Request	X	X				
	Central Budget	200X S Approved	X	X				
	Operational Plan	Organization Type 1	X	X	X			
	Operational Plan	Organization Type 2	X	X	X			
	Operational Plan	Partner Name	X	X	X			
	Operational Plan	Budget Information Related to Partners	X	X	X			
	Operational Plan	Mechanism Type	X	X	X			
	Operational Plan	USG Agency	X	X	X			
	Operational Plan	Mechanism Name	X	X	X			
	Operational Plan	Benefiting XXX Bureau	X	X	X			
	Operational Plan	Benefiting Country	X	X	X			
	Operational Plan	200X Op Plan - Initial	X	X	X			
	Operational Plan	200X Op Plan - Approved	X	X	X	X	X	
	Operational Plan	Key Issues	X	X	X	X	X	
	Operational Plan	OU Overview, Program Obj/Area/Element, Indicator, and Key Issue Narratives	X	X	X	X	X	
Operational Plan	Other OP Narratives not listed	X	X	X	X	X		
Operational Plan	Endorsement Memo	X	X					
Mission Strategic Plan	All Narratives	X	X					

*This is an illustrative list of data options. Each fiscal year may have a different set of data (e.g., FY 2008 had "653(a) Initial" and "653(a) Final," while FY 2007 did not). Furthermore, access to data related to interim steps in the budget process will be on a rolling basis (e.g., once FY 2009 Actual data is available, access to FY 2009 Estimate data will cease).

**The clearance procedures outlined in Section 6 must be followed prior to the dissemination of any data, including publicly available information.

Approved: Wade Warren, Deputy COO

Drafted: F/PM/SI/M&E – Nicholas Vivio, ext. 7-2698
Revised: F/PM/RA – Pat Sommers, ext 7-2605

Cleared:

F – Donna Stauffer
F – Khushali Shah
F – Lydia Hall
F – James Painter
L – Margaret Taylor
L – Oliver Lewis

ANNEX 2: 12 FAM 540

12 FAM 540 SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU)

*(CT:DS-117; 11-04-2005)
(Office of Origin: DS/SI/IS)*

12 FAM 541 SCOPE

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

- 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) 12958, as amended;

- (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 3490.1, dated May 8, 2002.
 - (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-117; 11-04-2005)

- 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 (LES), 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 engaged 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.