United States Department of State

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

Foreign Assistance Coordination and Tracking System (FACTS) Info

Data Use Policy

August 2014

Submitted by

Planning, Performance and System (F/PPS)

DOCUMENT CHANGE HISTORY

The table below identifies all changes that have been incorporated into this document.

Change #	Date	Version #	Description
N/A	May/08	Draft v1.0	FACTS and FACTS Info Data Use Policy Initial Working Draft
0001	June/08	Draft v2.0	Comments incorporated from Internal F/SIME Initial Review
0002	July/08	Draft v3.0	Comments incorporated from State/Legal Office
0003	August/08	Draft v4.0	Comments incorporated from Key Stakeholder Working Group
0004	October/08	Draft v5.0	Comments and clearance from F Senior Staff
0005	October/08	Final v1.0	Comments and clearance from F/PM
0006	November/08	Final v2.0	Comments and clearance from F/DCOO
0007	August/11	Final v3.0	Update to annex 1, 2, 3 and data use table
0008	May/13	Draft v6.0	Update to all sections and annexes
0009	July/13	Draft v7.0	Comments incorporated
0010	July/13	Final v4.0	Update to all sections and annexes
0011	June/14	Draft v1.0	Updates to Budget, Performance and Operational Plan sections and Annex1
0012	August/14	Final v4.0	Comments incorporated and cleared for updates

CLEARANCES:

Office of the Director of Foreign Assistance (F) – Vega, Dennis

USAID/MPBP – Crumbly, Angelique

USAID/PPL – Rader, Patricia

USAID/BRM – Napoli, Roman

S/Global Aids Coordinator – Gehron, Michael

L/LFA - Scott, Lela

TABLE OF CONTENTS

LIST OF ANNEXES

GLOSSARY OF TERMS USED IN THIS DOCUMENT

Contractor – U.S. Government personal service contractors who work for USAID or State.

Data –For the purposes of this document, data refer to both numbers and narratives in FACTS Info modules.

Implementing Partner – Organization contracted to implement foreign assistance activities for USAID, State, or other U.S. government agencies with data in FACTS Info.

Implementing Mechanism - Means of implementing a program or project to achieve identified results, generally through the use of a legally binding relationship established between an executing agency (generally a U.S. government agency like USAID or a host government agency) and an implementing entity (contractor, grantee, host government entity, international organization) to carry out programs with U.S. government funding.

Locally Employed Staff – Staff (both host-country nationals and Americans living overseas) who work for U.S. missions overseas.

PEPFAR U.S. government Agencies – U.S. government agencies that partner with S/GAC to deliver or coordinate activities and/or programs, including the Department of Defense (DoD), the Department of Commerce (DoC), the Department of Labor (DoL), the Department of Health and Human Services (HHS), and Peace Corps.

Users – Anyone within USAID, State, or PEPFAR U.S. government agencies with access to FACTS Info.

1. INTRODUCTION

The U.S. Government is committed to the open government and aid transparency. The President's Executive Order -- Making Open and Machine Readable the New Default for Government Information states that "Government information shall be managed as an asset throughout its life cycle to promote interoperability and openness, and, wherever possible and legally permissible, to ensure that data are released to the public in ways that make the data easy to find, accessible, and usable. In making this the new default state, executive departments and agencies (agencies) shall ensure that they safeguard individual privacy, confidentiality, and national security."

The Department of State and USAID are committed to openness and have established multiple avenues to provide data to the public including ForeignAssistance.gov, Performance.gov, and Dollar for Results.

This document provides users with the ability to promote openness in a responsible manner. It is a guide to using and sharing data contained in the Foreign Assistance Coordination and Tracking System (FACTS Info). This policy applies to all FACTS Info users and to all data contained within the system without exception. FACTS Info data is defined as narrative and numerical information contained within the various modules.

For data not currently referenced in this policy, please contact FACTInfoSupport@state.gov for questions and clarification of use. This policy will be reviewed and updated regularly, if necessary, annually.

Questions/Requests for Assistance: If FACTS Info Users need assistance with FACTS Info data they should address their questions to FACTSInfoSupport@state.gov.

2. DATA SENSITIVITY AND RISK

FACTS Info contains Sensitive But Unclassified (SBU) and UNCLASSIFIED data. SBU information is generally exempt from public disclosure, and depending on the type of information, dissemination may be restricted even within the federal government. The SBU information included in FACTS Info and communications stemming from or in support of the system, 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 U.S. 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. UNCLASSIFIED data are considered as bearing no risk designation; therefore it is not classified and can be released without additional clearances. SBU data is considered to be of moderate risk

for the reasons outlined above and while it is not classified, it is necessary to clear SBU data for external use. The clearance process for release of SBU data is outlined in Section 6 of this document.

In compliance with the President's Executive Order on Open Data and with OMB memo M-13-13, the FACTS Info Data Use Policy outlines good stewardship of the data contained in FACTS Info as well as the review, validation, clearance and release of data in support of downstream information processing.

Note: The data records contained within FACTS Info may be subject to release under the Freedom of Information Act (FOIA). This policy is not intended to provide instructions about how to respond to FOIA requests. For the Department of State, information about FOIA can be found at http://www.state.gov/m/a/ips/ or by calling the Department of State's FOIA Hotline at 202-261-8484 (x48484). For USAID, information about FOIA can be found in Automated Directive System (ADS) 507 at http://inside.usaid.gov/ADS/500/507.pdf.

3. DATA IDENTIFICATION

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

3.1 Source

Reports, spreadsheets, and documents generated from FACTS Info must be labeled with source information. These labels will be automatically generated for all reports run from FACTS Info. Users must ensure that these labels are retained, as appropriate, in the reports and/or added to relevant documents when sharing them with others. In addition, if data obtained from FACTS Info originated from an external source and is cited as such within FACTS Info, the user is required to cite the original data source when using this information for official reports or public consumption.

3.2 Sensitivity Markings

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 U.S. government audiences must be marked "U.S. government Only – Not for Distribution".

4. DATA FOR INTERNAL U.S. GOVERNMENT USE

Much of the data included in FACTS Info is restricted to internal U.S. government use, which limits dissemination to U.S. government Direct Hire personnel and individuals who are performing official governmental functions on behalf of the U.S. government. However, not all data can be shared with all U.S. government audiences, and much of the data in FACTS Info cannot be shared outside the Department of State (State) and the U.S. Agency for International Development (USAID) without special authorization. PEPFAR data has a slightly broader

distribution to include their U.S. government partner agencies beyond State and USAID: Department of Defense (DoD), Department of Commerce (DoC), Department of Labor (DoL), Department of Health and Human Services (HHS), and Peace Corps.

The table in Annex I summarizes the data available in FACTS Info and the restrictions applicable to the various types of information and audiences.

There are certain restrictions on data for internal U.S. government use. All documents produced using 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 U.S. government requirements. Please refer to Annex 2 for guidance on procedures pertaining to SBU information.

In addition, F Operational Plan, the Evaluation Registry component of the Performance Plan and Report, and the PEPFAR Country Operational Plan data are considered to be procurement sensitive and pre-decisional budget data that is therefore considered SBU and subject to sharing restrictions as summarized in Annex 1. Other budget data is also pre-decisional and thus, also considered SBU. Please refer to Annex 1 to determine which types of data can be shared with which audiences and Section 6 for clearance procedures.

5. DATA FOR EXTERNAL USE

Data listed as "Public" in Annex 1 may be shared with other U.S. government agencies and outside the U.S. government. Data may be listed as "Public" and shared accordingly after it has been cleared by the Office of U.S. Foreign Assistance Resources (F), or for PEPFAR data, the Office of the Global AIDS Coordinator (S/GAC). Please refer to the clearance procedures described in Section 6 that are applicable in certain circumstances.

The State and USAID budget data that can be shared with the public without additional clearances is that which is included in the annual Congressional Budget Justifications (CBJs). Foreign Operations CBJs can be found at http://www.state.gov/f/releases/index.htm.

For the purposes of this Data Use Policy, only data listed as "Public" in Annex 1 may be shared with implementing partners, i.e. organizations or personnel outside the U.S. government contracted to carry out activities or programs for USAID, State, or PEPFAR U.S. government agencies.

6. CLEARANCE PROCESSES

Annex 1 of this document defines the levels of restriction that apply to sharing various FACTS Info data. Sections 4 and 5 of this document describe additional restrictions. All FACTS Info users are responsible for adhering to these requirements.

The Office of U.S. Foreign Assistance Resources is dedicated to increasing the use of data and the ability to share information responsibly. The following clearance procedures must be followed prior to sharing FACTS Info data with certain audiences. In all cases, prior to the

dissemination of information from FACTS Info, the responsible individual must ensure that it is accurate, final, that it reflects current Foreign Assistance policies and procedures, that it is appropriate for the situation/request, and is labeled as required. The clearance process is managed with the intention of sharing the maximum information possible.

6.1 Budget Data

As indicated in Annex 1, once budget data have been made public through the release of the annual Congressional Budget Justification (CBJ) it can be used without any formal clearance process. As stated above, it is the responsibility of the user to ensure that the data provided answer the question being asked and that the appropriate caveats and explanations are included. For users not familiar with foreign assistance budget data, we recommend that you ask your Development Planning Office or Bureau Planner for assistance in developing your report. F Points of Contact (POCs) are also available to assist.

If other pre-decisional budget data that are part of State, USAID, and the PEPFAR U.S. government agencies budget formulation process is not included in the CBJ, it may never be made public. Pre-Decisional budget data are for internal use only, and are part of the deliberative, decision-making process – and needs to be cleared before sharing outside of State and USAID.

6.1a Country Development Cooperation Strategies (CDCS)

CDCS budget data are generally SBU and are intended for internal State/USAID use only. Public versions of CDCS's are available without budget data and can be accessed through usaid.gov. For more information on this data, contact PPL or the relevant regional bureau at USAID.

6.2 Performance Data

Performance data in the Performance Plan and Report (PPR) are generally SBU and require certain clearances for use outside of State and USAID. Individual PPR reports are the vehicle through which Operating Units (OU) can give a frank assessment of their performance and associated challenges to Washington, and thus should be reviewed and validated prior to initiating a clearance process for release of information. Additionally, some data contained in the PPR are procurement sensitive and cannot be released publicly (e.g. planned evaluations in the Evaluation Registry).

Review and validation is the process by which PPR feedback is provided from USAID and State stakeholders to an OU on their PPR, and the PPR is updated as necessary per that feedback and re-submitted by the OU. The re-submitted PPR is then considered final.

PPR data are made available for State and USAID ***internal*** use after the review and validation process is complete, which generally occurs by April of the fiscal year following data submission. After review and validation is complete, **numeric** performance data are no longer considered SBU and are available for public use. To request that certain numeric data be restricted from public disclosure, an OU must list the applicable indicator number(s) in its Endorsement Memo requesting that they remain SBU, and specify the reason.

All narrative PPR data are generally considered SBU until cleared for external use per the following process. To clear **narrative or OU-identified SBU numeric PPR data for external State, USAID or public use**:

1) The requester should contact their relevant Development Planner, Bureau Planner or equivalent as the first point of contact for their clearance and explain the reason for the data request and the audience that seeks the data.
2) In addition to the protocols set out by that bureau to clear data, the bureau must take steps to assure that the PPR data requested is final and, if applicable, contact the OU for confirmation and/or further review. This is especially critical if the PPR Endorsement Memo notes data that should not be released to the public.
3) The bureau and/or the requester should make sure that the data is labeled appropriately and in consultation with legal counsel.

Additionally, if the narrative is **to be used for an audience outside the Executive Branch** -- including, Congress and GAO, a mandated report, or in testimony-- in addition to the above clearances, the bureau must also **include the F POC in their clearance process**, providing specific instruction on what aspect(s) of the PPR narrative requires F POC focus and clearance.

The F POC will review the data and provide clearance, taking into account:

1) Possible sensitivities (security, procurement, etc.);
2) Appropriateness to share the data with the identified audience (referencing Annex 1);
3) Alignment with current foreign assistance policies and procedures;
4) Assurance that the appropriate stakeholders are listed to clear as well; and
5) Determination if higher-level F clearance for sensitive or controversial data is necessary or if a data release approval memo for large data requests is necessary from the FACTS Info Executive Sponsor.

Please note information from the PPR is consolidated into the Annual Performance Plan/Annual Performance Report (APP/APR) that accompanies the annual CBJ, and highlights aggregated progress made for a small set of foreign assistance indicators. APP/APR performance data does not need additional clearances for public use as the data (numbers and narratives) are validated and cleared prior to inclusion in the CBJ.

Please also note that selected numeric performance indicator data from the PPR will be published in various public products, including on Department of State and USAID websites, Performance.gov, and sectoral reports to Congress.

6.2a USAID Forward Performance Data USAID Forward performance data provide USAID, State, and the public with information about progress made toward achieving USAID Forward Reforms. Quantitative indicator data and associated narratives are collected. USAID Forward **numeric result data** as well as **narratives are not generally SBU** and will be made publicly available after USAID's review and validation process. **Annual target data are generally SBU** until clearance is obtained through the appropriate USAID regional bureau or USAID Forward leadership. Data are tabulated by indicator for each operating unit and in summary form and are available at http://www.usaid.gov/usaidforward.

To clear **USAID Forward Target Data for public use**:

1) The requester should contact the USAID Forward Tiger Team and explain the reason for the data request and the audience that seeks the data.
2) The Tiger Team will make a recommendation to the USAID Forward Leadership Team and the relevant regional bureau or issue owner must take steps to assure that the data requested is final and, if applicable, contact the OU for confirmation and/or further review.
3) The bureau and/or the requester should make sure that the data is labeled appropriately and in consultation with legal counsel.

6.3 Foreign Assistance Operational Plan Data

The Foreign Assistance Operational Plan (OP) provides State and USAID with a tool that demonstrates integrated planning and execution of foreign assistance funds. The OP is an internal, deliberative plan that warrants administrative control and protection from public or other unauthorized disclosure. As such, the OP is generally SBU and requires certain clearances for use outside of State/USAID or with the public.

Upon approval by F, an Operating Unit's OP serves as an agreement on the planned use of foreign assistance funds. Once the OP is approved, it can be used for internal (USAID/State) planning purposes. Representatives of other U.S. government agencies represented in the OU or with a specific interest in the OU must request release of an OP from the respective Operating Unit. Please note: Supporting Documents except for the Signed OP Verification Statement are owned by the bureaus that require that reporting. Please consult those bureaus for appropriate data release guidelines and clearances.

Some OP data may be used with audiences outside the Executive Branch (such as Congress, a mandated report, or in testimony), in which case the bureau must also include the F POC in their clearance process (as defined by the bureau), providing specific instruction on what aspect(s) of the OP require F POC focus. The F POC will review the data and provide clearance, taking into account:

1) Possible sensitivities (security, procurement, etc.);
2) Appropriateness to share the data with the identified audience (referencing Annex 1);
3) Alignment with current foreign assistance policies and procedures;
4) Assurance that the appropriate stakeholders are listed to clear as well; and
5) Determination if higher-level F clearance for sensitive or controversial data is necessary or if a data release approval memo for large data requests is necessary from the FACTS Info Executive Sponsor.

6.4 PEPFAR Country Operational Plan and Semiannual/Annual Program Performance Data

Redacted versions of the Country Operational Plans (COPs) and a subset of the APR data are released to the public. In their un-redacted form, COPs and Semiannual & Annual Program Results (S/APR) provide PEPFAR U.S. government agencies with tools that demonstrate integrated planning and execution of the program using PEPFAR funds. In their un-redacted form, the COP and S/APR are internal strategic planning and reporting documents that warrant administrative control and protection from public or other unauthorized disclosure. As such, the

un-redacted COP and S/APR are generally SBU and require certain clearances for use outside of PEPFAR U.S. government agencies.

Upon approval by the Department of State's Office of the Global AIDS Coordinator (S/GAC), an Operating Unit's COP or S/APR serves as an agreement on the planned use of PEPFAR funds and the progress the program makes as a result of those funds. Once the COP or S/APR are approved, they can be used for internal (PEPFAR U.S. government agencies) planning and management purposes.

Some COP and S/APR data that are not publicly released may be used with audiences outside the Executive Branch (such as OMB, Congress, a mandated report, or in testimony), in which case the requesting agency or OU must include S/GAC in their clearance process, providing specific instruction on what aspect(s) of the COP and S/APR require S/GAC focus. S/GAC will review the data and provide clearance, taking into account:

1) Possible sensitivities (security, procurement, etc.);
2) Appropriateness to share the data with the identified audience (referencing Annex 1);
3) Alignment with current foreign assistance policies and procedures;
4) Assurance that the appropriate stakeholders are listed to clear as well; and
5) Determination if higher-level clearance for sensitive or controversial data is necessary or if a data release approval memo for large data requests is necessary from the Global AIDS Coordinator.

6.5 Requests from Offices of Inspector General (IG) and the Government Accountability Office (GAO)

It is the policy of State and USAID to provide the GAO with the information it needs to fulfill its statutory responsibilities in an expeditious manner. Thus, OP and PPR data may be released to the GAO as described below when the information is considered final.

The State GAO Liaison Office is responsible for conducting all State liaison activities with the GAO and for coordinating State responses to information requests. The State GAO Liaison Office appoints a lead POC for each GAO investigation. All requests for SBU documents or information must come in writing through the GAO Liaison Office or lead POC, must reference a GAO job code, and must be relevant to an official study. If a request for information does not refer to an investigation number and has not been coordinated through the GAO Liaison Office, then the request should be referred to the GAO Liaison.

USAID's Management Bureau, Office of the Chief Financial Officer, Audit Performance & Compliance Division (M/CFO/APC) is responsible for conducting liaison activities with the GAO related to coordinating USAID responses to GAO reports, closing audit recommendations, and scheduling entrance and exit conferences. All requests for information related to these activities must come through M/CFO/APC (gaomailbox@usaid.gov). At each entrance conference, the Mission or Bureau/Independent Office (B/IO) appoints an Audit Action Officer (AAO) for coordinating field work. All requests for information related to field work must come through the AAO, must reference a GAO job/engagement code, and must be relevant to an official engagement or review. If a request for information does not refer to a GAO

job/engagement code and has not been coordinated through the AAO, then the request should be referred to M/CFO/APC.

Within F, the OP Coordinator is the POC for all GAO Operational Plan requests, and the PPR Coordinator is the POC for all GAO Performance Plan and Report requests. All official GAO requests for OPs or PPRs should be directed to the coordinators via the FOperationalPlan@state.gov or PPR@state.gov general mail boxes. The coordinators will provide **hard copies** only to the GAO Liaison for GAO review. To help prevent misinterpretation of the products by the GAO reviewers, the final versions of the OPs and PPRs, as well as the related guidance and a cover sheet that explains the documents will be provided.

Because these documents are generally SBU, normally the GAO is permitted to read them on State or USAID premises, but is not given electronic copies or printed copies of documents to remove or distribute. More information and GAO FAQs with detailed State procedures are available on the State/GAO Liaison website: http://rm.s.state.sbu/GAO-Liaison/Pages/GAO-Liaison.aspx.

Because the IG offices are internal State and USAID offices, procedures are not the same as for the GAO. Upon their request, F will provide the State or USAID IG offices copies of OPs and PPRs in both electronic and hard-copy form. OP requests should be directed to FOperationalplan@state.gove and PPR requests should be directed to PPR@state.gov. The IG will be provided with final versions and a cover sheet to explain the documents and the information included. The relevant F-POC will be included on all communication regarding GAO and IG requests for information.

Annex 1

This table describes the level of restrictions for sharing FACTS Info data. The 'X' indicates the greatest amount of sharing possible. **Thus, data may be shared with the audience listed in the column that is marked by X and all of the columns to the left of that column**. All requirements and descriptions discussed in the main section of this document apply.

In cases in which data are not available to the public, these are generally considered SBU and 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 U.S. Government, the disclosure of which could harm such processes.

Please note that not all FACTS Info users will see all the data included here. Data in FACTS Info is available to users based on their user profile.

		Data Audiences (order based on level of restriction)*							
Category	**Data**	**Internal F**	**Internal F/BRM**	**State USAID**	**Other USG**	**Executive Office of the President/ OMB**	**Congress**	**Public**	**Conditions for dissemination outside of State/USAID**
Budget Data									
Central Budget	20XX Actual Base							X	
Central Budget	20XX Actual YYY Supp							X	
Central Budget	20XX Actual Total							X	
Central Budget	20XX Initial Actual							X	
Central Budget	20XX Actual Update							X	
Central Budget	20XX Estimate							X	Once CBJ has been released
Central Budget	20XX Estimate Non-Initiative			X					Once CBJ has been released
Central Budget	20XX Request Base							X	Once CBJ has been released
Central Budget	20XX Request							X	Once CBJ has been released
Central Budget	20XX Request Control Base			X					
Central Budget	20XX Request OCO Base							X	Once CBJ has been released
Central Budget	20XX Request Non-Initiative Base							X	Once CBJ has been released
Central Budget	20XX Request Non-Initiative							X	Once CBJ has been released
Central Budget	20XX CBJ Request Narratives							X	Once CBJ has been released
Central Budget	20XX 653(a)							X	Once final 653(a) levels have been provided to Congress

Category	Data	Internal F	Internal F/BRM	State USAID	Other USG	Executive Office of the President/ OMB	Congress	Public	Conditions for dissemination outside of State/USAID
Central Budget	20XX 653(a) Control			X					
Central Budget	20XX Control Base			X					
Central Budget	20XX MSP Mission Request Base			X					
Central Budget	20XX MSRP Mission Request Base			X					
Central Budget	20XX MRR Mission Request			X					
Central Budget	20XX Functional Roundtable Recommendations			X					
Central Budget	20XX Bureau Request			X					
Central Budget	20XX Bureau Unfunded Request			X					
Central Budget	20XX Bureau Request Total			X					
Central Budget	20XX BRM Recommendation		X						
Central Budget	20XX USAID Proposal Non-Initiative		X						
Central Budget	20XX USAID Proposal		X						
Central Budget	20XX F Team Recommendation	X							
Central Budget	20XX Bureau Non-Initiative Passback Base			X					
Central Budget	20XX Bureau Passback Base			X					
Central Budget	20XX Bureau Non-Initiative Passback			X					
Central Budget	20XX Bureau Passback Non-Initiative			X					
Central Budget	20XX Bureau Passback			X					

Category	Data	Internal F	Internal F/BRM	State USAID	Other USG	Executive Office of the President/ OMB	Congress	Public	Conditions for dissemination outside of State/USAID
Central Budget	20XX Bureau Non-Initiative Appeal			X					
Central Budget	20XX Bureau Appeal Non-Initiative			X					
Central Budget	20XX Bureau Appeal			X					
Central Budget	20XX Bureau Appeal Base			X					
Central Budget	20XX Revised Bureau Request Base			X					
Central Budget	20XX Revised Bureau Non-Initiative Request			X					
Central Budget	20XX Revised Bureau Request Non-Initiative			X					
Central Budget	20XX Revised Bureau Request			X					
Central Budget	20XX S Decisions			X					
Central Budget	20XX S Recommendation			X					
Central Budget	20XX OMB Submission					X			Once OMB Submission has been transmitted
Central Budget	20XX OMB Narratives					X			Once OMB Submission has been transmitted
Central Budget	20XX Passback		X						
Central Budget	20XX OMB Passback		X						
Central Budget	Difference 2010 vs S	X							
Central Budget	20XX NOA Control Base			X					
Country Development Cooperation Strategy (CDCS)	20XX Budget per Development Objective and SPSD			X					

Category	Data	Internal F	Internal F/BRM	State USAID	Other USG	Executive Office of the President/ OMB	Congress	Public	Conditions for dissemination outside of State/USAID
Operational Plan Data									
Central Budget	20XX OP Control Base			X					
Central Budget	20XX OP/CP Current Base			X					
Central Budget	20XX OP Approved Base			X					
Operational Plan	20XX Op Plan - Submitted			X					
Operational Plan	20XX Op Plan - Approved			X					See Section 6
Operational Plan	20XX Op Plan - Updated			X					See Section 6
Operational Plan	Implementing Mechanism Narratives			X					See Section 6
Operational Plan	Key Issue Narratives			X					See Section 6
Operational Plan	Environmental Compliance Report Narrative			X					See Section 6
Operational Plan	Implementing Mechanism Name			X					See Section 6
Operational Plan	Prime Partner Name			X					See Section 6
Operational Plan	Implementing Mechanism Type			X					See Section 6
Operational Plan	Implementing Mechanism Number			X					See Section 6
Operational Plan	U.S. GOVERNMENT Agency			X					See Section 6
Operational Plan	Benefiting Country			X					See Section 6
Operational Plan	Funding Allocation by Standardized Program Structure			X					See Section 6
Operational Plan	Funding Attribution by Key Issue			X					See Section 6
Operational Plan	Signed OP Verification Statement			X					See Section 6

Category	Data	Internal F	Internal F/BRM	State USAID	Other USG	Executive Office of the President/ OMB	Congress	Public	Conditions for dissemination outside of State/USAID
Performance Plan and Report Data									
	Mission Objective Narratives							X	See Section 6
	Indicator Data							X	See Section 6
	Key Issue Narratives							X	See Section 6
	Evaluation Registry Data			X					See Section 6
	Success Stories							X	See Section 6
	Full OU-specific Performance Plan and Report (PPR)			X					
USAID Forward Data	Indicator Data							X	See Section 6
	Indicator Based Narratives							X	See Section 6
Other									
Mission Resource Request	All Narratives			X					
Mission Resource Request	20XX MSRP Constrained			X					
Mission Resource Request	20XX MSRP Preferred			X					
Standard Reports	Standardized Program Structure							X	
Standard Reports	Key Issue list by Year							X	
Master Indicator List	Indicator Lists and Reference Sheets							X	

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

ANNEX 2: 12 FAM 540

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.