United States Agency for International Development (USAID)

Bureau for Management/Office of the Chief Information Officer (M/OCIO)

GLOBAL ACQUISITION & ASSISTANCE SYSTEM (GLAAS) WASHINGTON USER ACCESS POLICIES AND FORMS PACKET

Version 4.0

March 28, 2014

DOCUMENT CHANGE HISTORY

The table below identifies all changes that have been incorporated into this document. Baseline changes require review and approval.

Change #	Date	Version #	Description
N/A	December 11, 2006	1.0	Draft document provided to USAID/OAA for comments.
1	February 28, 2008	2.0	Updated/revised to reflect USAID/OAA client input.
2	November 7, 2008	3.0	Updated/revised to reflect new roles and role changes.
3	March 28, 2014	4.0	Updated/revised to reflect new roles and role changes.

TABLE OF CONTENTS

List of Tables

1. GLAAS USER ACCESS POLICIES AND PROCEDURES

The purpose of this packet is to provide a central location for United States Agency for International Development (USAID) processes and forms required by Washington users who need access to the Global Acquisition System (GLAAS). This document also contains information and the necessary forms needed for Phoenix access, which is interfaced with GLAAS for committing and obligating funds, as well as the necessary form required for obtaining access to Business Objects Enterprise (BOE) for generating reports outside of the GLAAS application. Access to the various E-Gov systems is also addressed in this document. All required forms mentioned can be found in Appendix C. Role descriptions for both GLAAS and Phoenix can be found in Appendix B.

1.1 ACCESS TO GLAAS

GLAAS contains sensitive information that must be acquired, maintained, and reported in a secure manner. The User Access policy for GLAAS has been designed with the intention of ensuring protection of procurement sensitive information from disclosure under the Procurement Integrity Act (41 U.S.C. §423, implemented at FAR 3.104) and other applicable federal laws including the Privacy Act of 1974. The Privacy Act of 1974 prevents the disclosure of any record (e.g., any information regarding an individual's address, phone number, social security number, bank account number) to any person or agency without the written consent of the individual to whom the record pertains.

Access to GLAAS is controlled through the use of an application-level user ID and password, which is assigned once a user is authorized. To safeguard this data from unauthorized access, Agency security policy requires that access be restricted to comply with the above-mentioned laws. Accordingly, the following is a list of categories of personnel who may be granted access to GLAAS:

- U.S. Direct Hires (USDH) – Agency-employed U.S. citizens that consist of civil service and Foreign Service employees appointed under statutory authorities.
- Foreign Service National (FSN) Direct Hires – Non-U.S. citizen employees appointed under the authority of the Foreign Affairs Act of 1961.
- U.S. Personal Services Contractors (PSCs) – One of the primary sources of specialized assistance available to managers in designing and implementing development assistance programs and in providing administrative support.
- FSN PSCs – Foreign national PSCs employed by USAID.
- Third Country National (TCN) PSCs – Expatriate foreign nationals who are employed by USAID in a third country (a country other than the U.S. or the individual's country of origin), and who are employed under a personal services contract.
- Participating Agency Service Agreement (PASA); Participating Agency Program Agreement (PAPA); and Resource Support Service Agreement (RSSA) USDHs from other Agencies – PASAs, PAPAs and RSSAs are agreements between United States Government (USG) agencies that form the basis for detailing personnel.

- Detail-Ins from another Federal Agency – USDH employees detailed from other agencies.
- Technical Advisors in Aids, Child Survival and Population (TAACs) from another Federal Agency – Program-funded technical specialists who may be assigned direct hire duties and responsibilities.
- Presidential Management Fellows (PMFs) – A civil service program run by the Office of Personnel Management (OPM) that allows talented young professionals to work in USAID.
- Intern Investment Program – A new structured summer program that allows the Agency to identify candidates for the Foreign Service International Development Intern program.
- New Entry Professional (NEP) Program – USAID’s program for bringing well-qualified applicants into the Agency’s Foreign Service.

The following is a list of those personnel categories that will not normally be granted access to GLAAS because of the need to safeguard procurement sensitive information from non-government sources:

- All Fellows including, but not limited to, the following:
  - American Academy for the Advancement of Science (AAAS) Fellows
  - Population Fellows (POFP)
  - Stars Fellows
  - Joint Career Corps (JCC)
  - Public Health Institute (PHI)
- Intergovernmental Personnel Act (IPA)
- Institutional Contractors
- Short-term Purchase Order individuals

1.2 WAIVERS

Should the person requesting access to GLAAS fall into one of the non-approved personnel categories listed above, they must obtain a waiver. Requesting individuals should complete the *Approval Form for Access to GLAAS Production for Non-Authorized Users (Waiver)* and *Non-Disclosure Agreement for GLAAS Access (Waiver)* (see Appendix C). The waiver will be granted subject to the final approval of the GLAAS Information Systems Security Officer (ISSO) and the Executive Sponsor of GLAAS. The signing official attests that he/she has weighed carefully the risks of granting GLAAS access to the person requesting it, and that the waiver is acceptable, resulting from significant operational necessity.

1.3 USER ACCOUNT ACCESS AND ROLES REQUESTS

Requests for *account creation, role changes*, and *site access* will be made as described in this section.

1.3.1 Account Creation

All GLAAS User Access requests should be submitted to the Bureau Transition Coordinators (BTC).

The *USAID GLAAS Access Agreement* must be signed by the user and the user's supervisor. The BTC will complete the *GLAAS User Access/Roles Request Form* based on the request received from the supervisor.

Once a request has been received, the BTC reviews the GLAAS User role descriptions matrix (see Appendix B) to assist him/her in assigning or changing roles. In addition, the BTC must ensure that there are no conflicting role assignments and that a segregation of duties is maintained (i.e., a user cannot be assigned both the Program Manager (PM) and the Agreements Officer(AO)/Contracting Officer (CO)/Obligation Recorder (OR)/Purchase Card Holder (PCH) roles). Also, a user should not serve as an Agreement Officer, Contracting Officer and a Contracting/Agreement Officer Representative (COR/AOR) on the same action.

The BTC also verifies compliance of the request with access policies and then routes the completed package to the GLAAS Access Forms mailbox via e-mail to GLAASAccessForms@usaid.gov.

Once the forms are received, the GLAAS Access team will create user accounts in GLAAS based on the received request form and signed documents. A GLAAS user ID will be created based on the user's e-mail address (e.g., e-mail address:cagreen@usaid.gov – GLAAS user ID: cagreen).

Copies of all forms collected will be maintained by the GLAAS Access Team in Washington.

Note: First-time GLAAS users are required to complete all of the applicable forms and read the *USAID Rules of Behavior for Users*. User IDs and passwords will be issued only to those users who have had GLAAS Training in at least one of the training modules that matches their function(s) indicated on the role section of the *GLAAS User Access/Roles Request Form*. Validation of the user's training should be done by the GLAAS Access team prior to creating a user account.

1.3.2 Contracting/Agreement Officer Representative (COR/AOR) Role Assignment

For users requesting the COR/AOR role, the user must complete the on-line accruals course referenced in the General notice date 10/03/2007 before the role will be assigned. When possible, a copy of the course certificate and a valid copy of the user's COR/AOR certification should be given to the BTC before the role is assigned. The document should be included with the request submitted by the BTC to the GLAAS Access team.

1.3.3 Warrants Levels/Credit Card Thresholds

Users requesting the AO, CO, OR or Purchase Card Holder (PCH) role, the user must provide to his/her BTC the warrant level, amount and/or Purchase Card threshold. The information will be validated with the M/OAA Purchase Card Agency Program Coordinator and the M/OAA Office of Evaluation Office by the GLAAS Access Team.

1.4 GLAAS ROLE, DOCUMENT AND SITE ACCESS CHANGES/ADDITIONS

Users requesting changes/additional roles and/or document/site access must submit a request to the BTC. The BTC must send an e-mail to the GLAAS Access Team (GLAASAccessForms@usaid.gov) requesting the needed access based on the request received from the individual's supervisor. The GLAAS Access Team will file a copy of the e-mail request with the user's access forms.

1.5 DEACTIVATE GLAAS USER ACCOUNTS

GLAAS user accounts will be deactivated for the following reasons:

- User separation from USAID.
- User has received a new password that has not been used within 3 days of issuance.
- User fails to log into the system after 90 days.
- User participated in an event or demonstrated a pattern of behavior that suggests an unwillingness or inability on the part of the user to protect sensitive or classified information.

Users and supervisors must contact their BTC concerning any user account changes. The BTC must then submit an e-mail request to the GLAAS Access Team. User access privileges will be revoked within 2 days of the user's departure or when the determination has been made that a user no longer requires access to GLAAS.

1.6 TRANSFERRING GLAAS USERS

The user contacts their BTC via e-mail about their transfer prior to leaving. The user's BTC at the current location contacts the GLAAS Access Team within two days of the departure date so the GLAAS user account can be deactivated. On arrival, the BTC at the new location will complete the *GLAAS User Access/Roles Request Form* and send (via e-mail) the forms to the GLAAS Access Team. The GLAAS Access Team updates the user's information in the system.

1.7 PASSWORD RESET REQUESTS

All BTCs will be given the rights to reset passwords for their respective bureaus. The BTC should receive a formal request and the user must present a picture ID for verification in order for a password to be reset. The BTC will reset the user's password(s), notify the user via E-mail that the password has been reset, and provide the new password to the user via telephone.

1.8 TEMPORARY SYSTEM/SITE ACCESS

Users on travel to sites outside of their home site must contact the BTC (if on TDY to a Washington office) or local Mission POC (if on TDY to a Mission) at the temporary duty travel (TDY) location for access. The BTC (if on TDY to a Washington office) or local Mission POC (if on TDY to a Mission) must follow the same process for receiving account access for the TDY user except that a new user ID will not be created. The user will be given access to the TDY site.

Note: When completing the *GLAAS User Access/Roles Request Form*, the BTC (if on TDY to a

Washington office) or local Mission POC (if on TDY to a Mission) must list the duration for the TDY access. Once the TDY is complete, the user's TDY site access will be removed.

1.9 USER ACCESS AND ROLES VALIDATIONS

Role assignments in GLAAS equate to access rights to manipulate (create/update/delete) or read data for which a given user has authority, responsibility and/or accountability. These transactions must be done by the party who has the responsibility for, accountability of, and authority to conduct those transactions. Obviously, Agency managers are responsible and accountable for authorities they delegate. Therefore, GLAAS roles must be carefully reviewed prior to assignment and should not be expeditiously requested.

For the reasons stated above, Assistant Administrators have ultimate responsibility for GLAAS User Access and role assignments within their respective Bureaus. To this end, Assistant Administrators are strongly encouraged to review all users and assigned roles on at least a quarterly basis to ensure that roles and user IDs are current and valid for each user.

Violation of the above policy shall be enforced by penalties ranging from, but not limited to, an official reprimand, and permanent documentation of said reprimand, to permanent dismissal from USAID employment. Violations related to GLAAS security will be immediately reported to the USAID's Inspector General's Office.

BTCs, however should review the information on a monthly basis. Each month a report will be distributed via e-mail to each BTC for review and validation of all users and their respective roles. The reports should be reviewed for any changes, adjustments, or deletions. BTCs must review and submit to the GLAAS Access Team via e-mail any changes within five (5) days of receipt of the report.

1.10 REQUIRED FORMS FOR GLAAS SYSTEM ACCESS

The following forms, which are required for GLAAS system access, are included in Appendix C:

- USAID GLAAS Access Agreement
- GLAAS User Access/Roles Request Form
- Approval Form For Access to GLAAS Production for Non-Authorized Users (Waiver)
- Non-Disclosure Agreement for GLAAS Access (Waiver)

2. PHOENIX SYSTEM ACCESS PROCEDURES

Various roles in GLAAS require a corresponding Phoenix role to complete the financial interface required for various GLAAS processes. See the role descriptions for additional information about Phoenix roles. The GLAAS Access Team will be responsible for coordinating with the Phoenix Security Team (if necessary).

The signed *Phoenix Access Request Acknowledgement* form and *GLAAS User Access/Roles Request Form* should be submitted to the GLAAS Access Team via e-mail. The GLAAS Access Team will coordinate with the Phoenix Security Team to create, update, or deactivate Phoenix user accounts via e-mail. Once a Phoenix user account has been created, updated, or deactivated, the Phoenix Security Team will notify the GLAAS Access Team. The GLAAS Access team will respond to the BTC when the request has been completed.

The *GLAAS User Access/Roles Request* form is also required for Phoenix role changes.

Note: Phoenix user accounts are maintained by the Phoenix Security Team located in USAID Washington. The current process for obtaining Phoenix user accounts is followed, however as mentioned above, the *Phoenix Access Request Acknowledgement* form and *GLAAS User Access/Roles Request Form* provided in Appendix C must be used for GLAAS.

3. OTHER SYSTEM ACCESS

Users of GLAAS may require access to other systems during day-to-day operations. The following information is provided to assist users if they need to gain access to one of these systems.

3.1 E-GOV SYSTEM ACCESS

Each of the following E-Gov systems has an online self-registration process. Users needing accounts for any of these systems should refer to the M/OAA Solutions Center website for additional information (http://inside.usaid.gov/M/OAA/SolutionsCenter/egov/index.html):

- FedBizOpps (FBO) – http://inside.usaid.gov/M/OAA/SolutionsCenter/egov/fedbizopps.html
- Grants.gov – http://inside.usaid.gov/M/OAA/SolutionsCenter/egov/grants.html
- Contractor Performance System (CPS) – http://inside.usaid.gov/M/OAA/SolutionsCenter/pastperf/cps_perf.html
- Past Performance Information Retrieval System (PPRIS) – http://www.ppirs.gov/
- Electronic Subcontracting Reporting System (eSRS) – http://www.esrs.gov/

Note: Federal Procurement Data System-Next Generation (FPDS-NG)—USAID negotiators will use one standard user account to access FPDS-NG. However, COs will need to have a user ID and password assigned. User IDs will be provided to the contracting officers when they are initially set up in GLAAS.

3.2 BUSINESS OBJECTS ENTERPRISE ACCESS (EXTERNAL REPORTING)

Users needing access to the external reporting tool should complete the *Business Objects Enterprise Access Form* and submit the form to their BTC. The BTC will forward the form via e-mail to the CIO-Helpdesk-USAID with the stated approval in the body of the e-mail.

Note: BOE user accounts are maintained by the BOE Administrator located at USAID Washington.

4. GLAAS WASHINGTON USER PROCESS AND CHECKLISTS

BTCs at each of the bureau sites will be the first point of contact (POC) for GLAAS users in a bureau for user access-related requests.

The GLAAS Access Team is responsible for creating, maintaining, and deactivating GLAAS user accounts. Maintaining user accounts also includes updating user roles, and updating user site access and document sharing privileges.

The following checklists are used for completing the requested task(s) associated with access to the GLAAS system:

- GLAAS – New User Account Checklist
- GLAAS – Deactivate User Account Checklist (USAID/Washington)
- GLAAS – User Account Transfer Checklist
- GLAAS – User Account Password Reset Checklist

Table 4-1 identifies the forms that are associated with each checklist. These checklists are described in more detail in the sections that follow. The forms referenced in this section can be found in Appendix C.

Table 4-1. USAID/Washington Checklist/Form Matrix

Checklist Name	USAID GLAAS Access Agreement Form	GLAAS User Access/Roles Request Form	Approval Form for Access to GLAAS Production for Non-Authorized Users (Waiver) Form	Non-Disclosure Agreement for GLAAS Access (Waiver) Form	Phoenix Access Request Acknowledgement Form	Business Objects Enterprise Access Form
New User Account Checklist	Yes	Yes	Verify	Verify	If needed	If Needed
Deactivate User Account Checklist *	No	No	No	No	No	No
User Account Transfer Checklist	No	Yes	No	No	If needed	No
User Account Password Reset Checklist **	No	No	No	No	No	No

*An e-mail should be sent to the GLAAS Access Team mailbox by the BTC.

**An e-mail should be sent to the BTC by the user.

4.1 GLAAS NEW USER ACCOUNT CHECKLIST

Table 4-2 identifies the steps required to request a new user account on the GLAAS system.

Table 4-2. GLAAS New User Account Checklist

Step	POC	Description
1	BTC	Download the *USAID GLAAS Washington User Access Policies and Forms Packet* at: http://inside.usaid.gov/glaas/index.php?q=node/62
2	User	Complete and sign the *USAID GLAAS Access Agreement* form. Users are encouraged to take this form with them to training so that the form can be signed by the GLAAS trainer.
3	User	If needed – complete and sign the *Phoenix Access Request Acknowledgement* form.
4	User	If needed – complete and sign the *Business Objects Enterprise Access Form*.
5	User	Read the *USAID Rules of Behavior for Users*, file name: 545mbd_060106_cd44 - http://inside.usaid.gov/ADS/500/545mbd.doc
6	CORs only	Completion of the on-line Accruals course is required before access will be given. In addition, a copy of COR Certification and Accruals training certificate should be included with the completed GLAAS User Account documentation (if available).
7	Supervisor	Sign the *USAID GLAAS Access Agreement form*. (other forms if needed)
8	Supervisor	Validate that the user received/reviewed *USAID Rules of Behavior for Users* document.
9	Supervisor	(WAIVER) Required for non-authorized employees only (see Section 1.2) – Complete and sign the *Approval Form for Access to GLAAS Production For Non-Authorized Users (Waiver)* document.
10	Supervisor	(WAIVER) Required for non-authorized employees only (see Section 1.2) – Complete and sign the *Non-Disclosure Agreement for GLAAS Access (Waiver)* document.
11	BTC	Confirm the user has received GLAAS Training and verify compliance of user requests with access policies.
12	BTC	Complete *GLAAS User Access/Roles Request Form*.
13	BTC	Send all of the signed and completed forms to the GLAAS Access team. Submit as a scanned PDF file via email.
14	GLAAS ISSO	The GLAAS ISSO reviews the new user access/roles request package and approves or disapproves the request.
15	GLAAS Access	Review the submitted user account request forms for accuracy and completion.

Step	POC	Description
16	GLAAS Access	Forward the signed and completed forms for the respective systems to the Phoenix/Warrants teams (as needed).
17	GLAAS Access	Create GLAAS (PRISM) user account for the user.
18	GLAAS Access	Create FPDS-NG user account for the user (as needed).
19	GLAAS Access	Notifies via e-mail the BTC that the GLAAS (PRISM), and FPDS-NG, user IDs (only user IDs) have been created.
20	GLAAS Access	Send ONLY the USER a second e-mail – identifying the GLAAS (PRISM) initial passwords. **Note**: The user will be able to access GLAAS but will not be able to run reports or perform any financial transactions until she/he is given BOE and Phoenix access.
21	GLAAS Access	The GLAAS Access Team stores all of the user access forms.

4.2 GLAAS DEACTIVATE USER ACCOUNT CHECKLIST (USAID/WASHINGTON)

Table 4-3 identifies the steps required to Deactivate a user account on the GLAAS system.

Table 4-3. GLAAS Deactivate User Account Checklist (USAID/Washington)

Step	POC	Description
1	Supervisor or M/IRM	Notifies the BTC about the need to deactivate user's access rights.
2	BTC	BTC sends (via e-mail) the GLAAS Access Team the user's account information.
3	GLAAS Access	Deactivates the user's access rights.
4	GLAAS Access	Notifies (via e-mail) the System Administrator for Phoenix about the deactivation of the user's access rights (as needed).
5	Phoenix System Administrator	Deactivates user's Phoenix Account.
6	Phoenix System Administrator	Notifies (via e-mail) the GLAAS Access Team of the account deactivation.
7	GLAAS Access	Stores the account deactivation email sent by the BTC.

4.3 GLAAS USER ACCOUNT TRANSFER CHECKLIST

Table 4-4 identifies the steps required to transfer a user account on the GLAAS system.

Table 4-4. GLAAS User Account Transfer Checklist

Step	POC	Description
1	User	Contacts and informs his/her BTC about the transfer.
2	BTC	Contacts the GLAAS Access Team within two days of the user's departure date.
3	GLAAS Access	Deactivates the user's GLAAS account.
4	New Site BTC/POC	On user's arrival, the new BTC/POC completes the *GLAAS User Access/Roles Request Form*.
5	New Site BTC/POC	The BTC/POC sends (via email) the forms to the GLAAS Access Team.
6	GLAAS Access	Updates the GLAAS user's account.
7	GLAAS Access	Sends the Phoenix user access forms to the Phoenix System Administrators (if necessary).
8	Phoenix System Administrator	Updates the user's Phoenix account.
8	Phoenix System Administrator	Notifies (via email) the GLAAS Access Team that the account has been updated.
9	GLAAS Access	Stores all of the user access forms.

4.4 GLAAS USER ACCOUNT PASSWORD RESET CHECKLIST

Table 4-5 identifies the steps required to request a password reset for an account on the GLAAS system.

Table 4-5. GLAAS User Account Password Reset Checklist

Step	POC	Description
1	User	Contacts their BTC and presents a valid picture ID.
2	BTC	Resets the user's password.
3	BTC	Notifies the user (via email) that their password has been reset.
4	BTC	Provides the user with the new password via telephone.

APPENDIX A: ACRONYMS

Acronym	Definition
AAAS	American Academy for the Advancement of Science
AO	Agreement Officer
AOR	Agreement Officer Representative
APS	Annual Program Statement
BOE	Business Objects Enterprise
BTC	Bureau Transition Coordinator
CO	Contracting Officer
COR	Contracting Officer Representative
CPS	Contractor Performance System
eSRS	electronic Subcontracting Reporting System
FAR	Federal Acquisition Regulation
FBO	FedBizOpps
FPDS-NG	Federal Procurement Data System - Next Generation
FSN	Foreign Service National
GLAAS	GLobal Acquisition & Assistance System
IAA	Interagency Agreement
ID	Identification
IPA	Intergovernmental Personnel Act
IRM	Information Resources Management
ISSO	Information Systems Security Officer
JCC	Joint Career Corps
M/OCIO	Management Bureau/Office of the Chief Information Officer
M/OAA	Management Bureau/Office of Acquisitions and Assistance
M/OAA/CAS	Management Bureau/Office of Acquisitions and Assistance/Cost, Audit and Support Division
N/A	Not Applicable
NEP	New Entry Professional
OPM	Office Personnel Management
OR	Obligation Recorder
PAPA	Participating Agency Program Agreement

Acronym	Definition
PASA	Participating Agency Service Agreements
PCH	Purchase Card Holder
PDF	Portable Document Format
PHI	Public Health Institute
PM	Program Manager
PMI	Presidential Management Interns
POC	Point of Contact
POPF	Population Fellows
PPRIS	Past Performance Information Retrieval System
PRIME	Principal Resource for Information Management Enterprise-Wide
PSC	Personal Services Contractors
RFA	Request for Application
RSSA	Resource Support Service Agreements
SA	System Administrator
SME	Subject Matter Expert
TAAC	Technical Advisors in Aids, Child Survival and Population
TCN	Third Country National
TDY	Temporary Duty Travel
USAID	U.S. Agency for International Development
USAID/W	U.S. Agency for International Development/Washington
U.S.C	United States Code
USDH	United States Direct Hire
USG	United States Government

APPENDIX B: GLAAS USER ROLE DESCRIPTIONS

GLAAS Role	USAID Role	Definition	Restrictions	Class Requirements	Phoenix Role
Requestor	Program Analyst Requestor Activity Manager Contracting/Agreement Officer's Representative (COR/AOR)	A person who has rights to create and modify a request. Within GLAAS, the Requestor role has the ability to create and self-approve the APP, prepare request packages, attach all documentation (Statement of Work (SOW), Budget, etc.), edit/modify (check in and check out) all documentation, and draft pending commitments.	User cannot be assigned the following roles: FMO	GLAAS 101 Requesting	Procurement Commitment Verifier (PCVERIFYR)
Program Manager	Budget Authority Project Team Lead Strategic Objective Team Leader Office Director Controller	The person responsible for approving and committing the funds. Within GLAAS, the Program Manger role assigns the Buyer and approves the requisition (which will create a commitment in Phoenix).	User cannot be assigned the following roles: Contracting Officer/ Agreement Officer Purchase Card Holder FMO	GLAAS 101 Requesting	Procurement Commitment Processor (PCPROCR)
Contracting Officer/ Agreement Officer	Contracting Officer Agreement Officer EXO Deputy Mission Director Mission Director Administrator Deputy Administrator	An individual who has a warrant or is authorized to obligate funds and approve A&A and Interagency Agreement (IAA) awards. The CO/AO has the authority to enter into, administer, and terminate contracts, grants, and cooperative agreements. The CO/AO role within GLAAS is responsible for managing Buyer Workload, reporting to the Federal Procurement Data System-New Generation (FPDS-NG) and Federal Assistance Award Data System (FAADS) where applicable. Also approving solicitations & awards and obligating funds in Phoenix.	User cannot be assigned the following roles: Program Manager FMO	GLAAS 102 Buying GLAAS 106 Sr. Management (For Mission Directors, Administrators and Deputy Mission Directors, and Deputy Administrators only who may execute an obligation for a Mission Director and Administrator warrant)	Procurement Obligation Processor (POPROCR)

GLAAS Role	USAID Role	Definition	Restrictions	Class Requirements	Phoenix Role
Agreement Officer Only (AO Only)	Agreement Officer	A person within the agency who is authorized to obligate funds and approve Assistance Awards and Inter-Agency Agreements, but does not have authority to approve Acquisition Awards. The Agreement Officer role has the authority to enter into, administer, and terminate Grants, Cooperative Agreements, and IAAs; this user does not have parallel authority for contracts. The AO role within GLAAS is responsible for managing Buyer Workload, reporting to FAADS and approving Assistance Awards and IAAs, thereby obligating funds in Phoenix.	User cannot be assigned the following GLAAS roles: Program Manager Contracting Officer FMO	GLAAS 102 Buying	(POPROCR)
A&A Specialist	Contract Specialist Negotiator A&A Specialist Buyer Procurement Agents Procurement assistants	Acquisition and Assistance role that is responsible for preparing solicitations, synopses, requests for applications, and award packages, as well as preparing solicitation notices, synopses, and award notices to FedBizOpps or Grants.gov and creating Federal Procurement Data System – New Generation (FPDS-NG) reports. A Buyer/Negotiator also handles contract negotiations.	User cannot be assigned the following roles: FMO	GLAAS 102 Buying	Procurement Obligation Verifier (POVERIFYR)
Obligation Recorder (OR)	Authority to serve as the Obligation Recorder in GLAAS will be limited to positions with the appropriate level of responsibility, such as Project Officers, Program Managers, Team Leads, or equivalent positions	The user creates, updates, and approves inter-agency agreements (IAAs) and grants in the system; generally assuming the delegation of authority, threshold or warrant of the user that they represent (i.e., Administrator). The OR creates the obligation on behalf of a non-OAA authorized obligator and does not have obligation authority or warrant authority (Pursuant with ADS 300). Authority to serve as the Obligation Recorder in GLAAS will be limited to positions with the appropriate level of responsibility, such as Project Officers, Program Managers, Team Leads, or equivalent positions.	User cannot be assigned the following GLAAS roles: Program Manager FMO Delegation of Obligation Recorder duties is neither mandatory nor encouraged. All AAs/DAAs with Warrant authority should be training in GLAAS 106 and have access to GLAAS in order to obligate funds. No new Obligation Recorders will be approved for any office or Bureau.	GLAAS 102 Buying	POPROCR

GLAAS Role	USAID Role	Definition	Restrictions	Class Requirements	Phoenix Role
Purchase Card Holder	Purchase Card Holder (PCH)	The Purchase Card is a streamlined procurement method that saves time and administrative costs. In GLAAS, Purchase Card Holders can create and approve (within their limited delegated authority) Purchase Card Orders.	User cannot be assigned the following roles: Program Manager FMO	GLAAS 103 Purchase Cards NOTE: If a user has taken BOTH 101 Requesting and 102 Buying they are not required to take this course for the role.	POPROCR
BTC Site Administrator	GLAAS BTC Site Administrator	The user is a GLAAS Subject Matter Expert who is responsible for resetting passwords, creating routing lists and reassigning Buyers in a Mission or Bureau. The Site Administrator also provides system and user support as it relates to GLAAS and coordinates with the Regional Site Administrator or GLAAS Solution Center for system and user support.	Users receiving this role must do so in conjunction with another role in GLAAS. Regional and Client Missions should designate up to 5users for this role per Mission/Client Office. User cannot be assigned the following roles: FMO	GLAAS 105 Site Administration	N/A

APPENDIX C: USAID GLAAS WASHINGTON USER ACCESS FORMS

This appendix contains the following USAID GLAAS Washington user access forms:

- USAID GLAAS Access Agreement
- GLAAS User Access/Roles Request Form
- Approval Form for Access to GLAAS Production for Non-Authorized Users (Waiver)
- Non-Disclosure Agreement for GLAAS Access (Waiver)
- Phoenix Access Request Acknowledgement
- Business Objects Enterprise Access Form

This Page Intentionally Blank

USAID GLAAS ACCESS AGREEMENT

This document outlines an agreement between the U.S. Agency for International Development (USAID) and an Authorized Individual (USER) requiring access to a computer application falling within the USAID Global Acquisition & Assistance System (GLAAS).

1. The USER agrees to abide by all USAID policies, procedures, and guidelines to protect USAID computer systems from misuse, abuse, loss, or unauthorized access.
2. The USER agrees to process only unclassified information.
3. The USER agrees to protect his/her unique user ID and password. Should the USER suspect compromise of his/her password or user ID, he/she will report the suspected compromise to his/her bureau/office GLAAS Liaison persons. The USER will change his/her password immediately upon suspicion of compromise.
4. The USER will NOT share user IDs or passwords. Writing down a user ID or password for personal use is PROHIBITED.
5. The USER agrees NOT to enter his/her user ID or password in a file or record maintained in any automated system.
6. The USER agrees to use/create a unique password consisting of a MINIMUM of twelve (12) alphanumeric characters for GLAAS. The USER will be prompted to change his/her password at least every ninety (90) days. USAID reserves the right to change a password or terminate access at any time.
7. The USER agrees to LOG OFF at any time the USER's terminal will be unattended by the USER.
8. The USER agrees to give immediate notification to his/her GLAAS Liaison persons when there is a change in the employee status eliminating the need to perform certain roles and/or when access to GLAAS is no longer required.
9. The USER agrees to abide in all respects by 41 U.S.C. 423, The Federal Procurement Policy Act (Act), and specifically agrees not to disclose source selection information or contractor bid or proposal information (as those terms are defined in the Act) to any person or entity, including persons or entities within the USER's employing contractor firm, not authorized by agency regulations or the Contracting Officer to receive such information; in addition, the USER specifically agrees not to knowingly obtain source selection information or contractor bid or proposal information prior to the award of a federal agency procurement contract to which the information relates when the USER has not been authorized by agency regulations or the Contracting Officer to receive such information.
10. The USER agrees to access only those roles within the selected GLAAS applications for which access authorization by the USAID was granted.
11. The USER agrees that information acquired from access to a Federal computer system may not be used for personal gain, profit, or publication or provided to any non-Federal organization without the PRIOR written approval of the USAID General Counsel.

I agree to abide by this agreement knowing that any violation of established USAID policy, procedures or guidelines may result in administrative action, civil or criminal prosecution, or termination of employment.

AGREEMENT		
PRINTED NAME	SIGNATURE	AGENCY/ OFFICE
BUSINESS ADDRESS	BUSINESS PHONE NUMBER	DATE
☐ I have read and agree to the USAID Rules of Behavior for Users.	☐ The USER has completed GLAAS courses signed and dated by Instructors below in full.	☐ The USER has completed the required on-line Accruals course (COTRs ONLY)

SUPERVISOR'S SIGNATURE:

INSTRUCTOR: For each course completed, print name and provide date of completion below

GLAAS TRAINING COURSES:	☐ 101 Requesting ____	☐ 103 Purchase Card ____
	☐ 102 Buying ____	☐ 104 FMO Review ____
	☐ 105 Site Admin ____	☐ 106 Senior Management ____

PRIVACY ACT STATEMENT	
AUTHORITY	50 U.S.C 402 (Note), E.O. 12333
PURPOSE	To allow the Agency to manage information pertaining to the User's PRINCIPAL Account.
ROUTINE USE	Dissemination within the U. S. Agency for International Development.
DISCLOSURE OF INFORMATION	Disclosure of this information is voluntary.
EFFECTS OF NOT PROVIDING	Failure to provide information requested could result in the inability of the Agency to provide the USER with a user ID and password.

This Page Intentionally Blank

GLAAS USER ACCESS/ROLES REQUEST FORM

Request Date: ____________

New User: ☐ **Current User:** ☐ **No Login Rights**[1]**:** ☐

USER NAME (LAST, FIRST)	PHONE NO.	EMAIL ADDRESS
GLAAS USER ID (USE E-MAIL ADDRESS)	**USER OFFICE SITE OR MISSION**	**AUTHORIZED WARRANT LEVEL/PURCHASE CARD THRESHOLD**
SUPERVISOR NAME	**SUPERVISOR PHONE NUMBER**	**AUTHORIZED BY (POC/BTC NAME)**

Employee Category

- ☐ USDH
- ☐ FSNDH
- ☐ FSNPSC
- ☐ USPSC
- ☐ TCNPSC
- ☐ RSSA/ PASA
- ☐ Detail-In (U.S. Govt.)
- ☐ TAACS
- ☐ PMI
- ☐ Intern

Waiver Required

- ☐ AAAS Fellows
- ☐ POPF Fellows
- ☐ Stars Fellows
- ☐ JCC
- ☐ IPA
- ☐ Institutional Contractors
- ☐ PO or Retired Employees

GLAAS Roles[2, 3] **[PHOENIX Roles]**

- ☐ **Requestor**
- ☐ **Program Manager**[2] [PCPROCR]

- ☐ **Agreements Officer/IAA Approver Only**[2] (all sec.org) [POPROCR]
- ☐ **Buyer** (Negotiator/A&A Specialist)[2] [POVERIFYR]
- ☐ **Contracting Officer / Agreements Officer**[2] (all sec.org) [POPROCR]
- ☐ **Obligation Recorder** (Grants & IAAs Only)[2] – Washington Only - (all sec.org) [POPROCR]
- ☐ **Purchase Card Holder**[2] [POPROCR]

- ☐ **Financial Management Officer** – Mission Only

- ☐ **Bureau Transition Coordinator** – Washington Only
- ☐ **Regional Site Administrator** – Mission Only
- ☐ **Local Site Administrator** – Mission Only

- ☐ **Approver -** OSDBU only
- ☐ **OAA Support**[4]
- ☐ **View Only**[4] – Washington Only

TDY Site Access

Start:

End:

LAC[5]

- ☐ **USAID/Dom Rep**
- ☐ USAID/Barbados
- ☐ **USAID/Jamaica**
- ☐ **USAID/El Salvador**
- ☐ USAID/G-CAP_REG[6]
- ☐ USAID/Guatemala
- ☐ USAID/Mexico
- ☐ **USAID/Honduras**
- ☐ **USAID/Nicaragua**
- ☐ **USAID/Peru**
- ☐ USAID/Brazil
- ☐ USAID/Ecuador
- ☐ USAID/Paraguay
- ☐ **USAID/Colombia**
- ☐ **USAID/Haiti**

AFR[5]

- ☐ **USAID/EA (East Africa)**
- ☐ USAID/CARPE
- ☐ USAID/DROC (Congo)
- ☐ USAID/Kenya
- ☐ **USAID/Rwanda**
- ☐ **USAID/Sudan**
- ☐ **USAID/Uganda**
- ☐ **USAID/SA (Southern Africa)**
- ☐ USAID/Angola
- ☐ USAID/Botswana
- ☐ USAID/Namibia
- ☐ **USAID/Madagascar**
- ☐ **USAID/Malawi**
- ☐ **USAID/Zimbabwe**
- ☐ **USAID/Senegal**
- ☐ **USAID/GUI-SL (Guinea / Sierra Leone)**
- ☐ **USAID/Mali**
- ☐ **USAID/Ghana**
- ☐ USAID/West Africa(WARP)
- ☐ **USAID/Benin**
- ☐ **USAID/Ethiopia**
- ☐ **USAID/Liberia**
- ☐ **USAID/Mozambique**
- ☐ **USAID/Nigeria**
- ☐ **USAID/South_Sud**
- ☐ **USAID/Tanzania**
- ☐ **USAID/Zambia**

ASIA[5]

- ☐ **USAID/India**
- ☐ USAID/Sri Lanka
- ☐ **USAID/Philippines**
- ☐ USAID/Mongolia
- ☐ **USAID/RDMA (THAILAND)**
- ☐ USAID/Burma
- ☐ USAID/Timor_Leste
- ☐ USAID/Vietnam
- ☐ **USAID/Cambodia**
- ☐ **USAID/AFG (Afghanistan)**
- ☐ **USAID/Bangladesh**
- ☐ **USAID/CAR**
- ☐ **USAID/Indonesia**
- ☐ **USAID/Pakistan**
- ☐ **USAID/Nepal**

ME[5]

- ☐ **USAID/Egypt**
- ☐ USAID/Lebanon
- ☐ USAID/Morocco
- ☐ USAID/Yemen
- ☐ **USAID/Iraq**
- ☐ **USAID/Jordan**
- ☐ **USAID/MERP**
- ☐ **USAID/WB GAZA**

E&E[5]

- ☐ **USAID/Georgia**
- ☐ USAID/Azerbaijan
- ☐ **USAID/Armenia**
- ☐ **USAID/Kosovo**
- ☐ **USAID/BIH (Bosnia-Her)**
- ☐ USAID/Albania
- ☐ USAID/Macedonia
- ☐ **USAID/SRB-MNE**
- ☐ **USAID/Ukraine**
- ☐ USAID/Belarus
- ☐ USAID/Cyprus
- ☐ USAID/Moldova

[1]Select this for a user to have a user ID, but not log in rights to GLAAS (i.e., COTRs that are not direct hires or do not have the waiver to access GLAAS but are identified on an award).
[2]Users with the Program Manager role cannot also have the Contracting Officer, Purchase Card Holder, Agreement Officer, Obligation Recorder, FMO role(s), or vice versa.
[3]Users needing access to any of the E-Gov systems, should refer to the OAA Solution Center E-Gov Web-site: http://inside.usaid.gov/M/OAA/SolutionsCenter/egov/index.html
[4]Users with the OAA Support or View Only role must complete the GLAAS Waiver forms regardless of the selected Employee Category.
[5]Contracting Officers (CO) / Agreements Officers (AO) will be granted all-site access in Phoenix.
[6]Only users from Guatemala and El Salvador should receive access to G-CAP_REG funds
[7]All GLAAS EGEE users are assigned to the EGEE GLAAS Site. Subcategories are necessary for Phoenix security purposes

rev. 14OCT2014

Washington Sites[5]

- ☐ A/AID
- ☐ AA/AFR
- ☐ AA/ASIA
- ☐ AA/DCHA
- ☐ AA/E+E
- ☐ AA/EGEE
- ☐ AA/GH
- ☐ AA/LAC
- ☐ AA/LPA
- ☐ AA/M
- ☐ AA/ME
- ☐ AA/PPC
- ☐ AFR
- ☐ ASIA
- ☐ ASIA/EAA
- ☐ ASIA/SAA
- ☐ ASIA/SPO
- ☐ ASIA/TS
- ☐ BFS
- ☐ DCHA
- ☐ DCHA/ASHA
- ☐ DCHA/CMM
- ☐ DCHA/CS3
- ☐ DCHA/DG
- ☐ DCHA/FFP
- ☐ DCHA/OFDA
- ☐ DCHA/OMA
- ☐ DCHA/OTI
- ☐ DCHA/PPM
- ☐ DCHA/PVCASHA
- ☐ DCHA/VFP
- ☐ E&E
- ☐ EGEE[7] (Also select office category)
  - ☐ EGEE/DC
  - ☐ EGEE/ED
  - ☐ EGEE/EI
  - ☐ EGEE/EP
  - ☐ EGEE/FAB
  - ☐ EGEE/GCC
  - ☐ EGEE/GEWE
  - ☐ EGEE/LTRM
  - ☐ EGEE/MPEP
  - ☐ EGEE/PDMS
  - ☐ EGEE/PLC
  - ☐ EGEE/TRR
  - ☐ EGEE/W
- ☐ EOP
- ☐ FA
- ☐ GC
- ☐ GH
- ☐ HR
- ☐ LAB
- ☐ LAC
- ☐ LPA
- ☐ LPA/CL
- ☐ LPA/PIPOS
- ☐ LPA/PL
- ☐ LPA/SCP
- ☐ M
- ☐ M/AS
- ☐ M/CFO
- ☐ M/CIO
- ☐ M/MPBP
- ☐ M/OAA
- ☐ M/OAA/BFS/ARP
- ☐ M/OAA/BFS/CMS
- ☐ M/OAA/CAS
- ☐ M/OAA/CAS/CAM
- ☐ M/OAA/CAS/OCC
- ☐ M/OAA/CAS/SUP
- ☐ M/OAA/DCHA
- ☐ M/OAA/DCHA/AFP
- ☐ M/OAA/DCHA/DOFDA
- ☐ M/OAA/DCHA/OTI
- ☐ M/OAA/E
- ☐ M/OAA/EGEE
- ☐ M/OAA/EGEE/DHWA
- ☐ M/OAA/EGEE/EMD
- ☐ M/OAA/EGEE/PEP
- ☐ M/OAA/GH
- ☐ M/OAA/GH/HSR
- ☐ M/OAA/GH/OHA
- ☐ M/OAA/GH/POP
- ☐ M/OAA/OD
- ☐ M/OAA/P
- ☐ M/OAA/RM
- ☐ M/OAA/SIDP
- ☐ M/OAA/T
- ☐ M/OAA/T/COM
- ☐ M/OAA/T/TRANS
- ☐ M/OMS
- ☐ ME
- ☐ ME/AMS
- ☐ ME/IR
- ☐ ME/MEA
- ☐ ME/SPO
- ☐ ME/TS
- ☐ OAPA
- ☐ OIG
- ☐ OIG/AIG/A
- ☐ OIG/AIG/I
- ☐ OIG/AIG/M
- ☐ OIG/AIG/MCC
- ☐ OSDBU/MRC
- ☐ OSDBU/OD
- ☐ PPC
- ☐ PPC/DCO
- ☐ PPC/P
- ☐ PPC/SPP
- ☐ PPL
- ☐ SEC/CIS
- ☐ SEC/ISP
- ☐ SEC/OD
- ☐ SEC/PSD

[1] Select this for a user to have a user ID, but not log in rights to GLAAS (i.e., COTRs that are not direct hires or do not have the waiver to access GLAAS but are identified on an award).
[2] Users with the Program Manager role cannot also have the Contracting Officer, Purchase Card Holder, Agreement Officer, Obligation Recorder, FMO role(s), or vice versa.
[3] Users needing access to any of the E-Gov systems, should refer to the OAA Solution Center E-Gov Web-site: http://inside.usaid.gov/M/OAA/SolutionsCenter/egov/index.html
[4] Users with the OAA Support or View Only role must complete the GLAAS Waiver forms regardless of the selected Employee Category.
[5] Contracting Officers (CO) / Agreements Officers (AO) will be granted all-site access in Phoenix.
[6] Only users from Guatemala and El Salvador should receive access to G-CAP_REG funds
[7] All GLAAS EGEE users are assigned to the EGEE GLAAS Site. Subcategories are necessary for Phoenix security purposes

APPROVAL FORM FOR ACCESS TO GLAAS PRODUCTION FOR NON-AUTHORIZED USERS (WAIVER)

Name of individual for whom access is requested:

____

Employing organization of above individual:

____

Instance to which access is requested:

____

Period for which access is requested:

____

Justification/rationale for access request:

____

____

____

____

Signature of U.S.D.H. requesting access:

____

Attachments:

______ USAID GLAAS Request Form

______ USAID GLAAS Access Agreement Form – signed by above the individual.

______ Non-Disclosure Agreement for GLAAS Access (Waiver) – signed by employing organization of above individual.

Approval/Disapproval by GLAAS ISSO

Approved: ________________________ Disapproved: _______________________

Conditions for Approval, if applicable:

____

____

____

This Page Intentionally Blank

NON-DISCLOSURE AGREEMENT FOR GLAAS ACCESS (WAIVER)

CONTRACTOR, ______________________ ("the Contractor"), has a signed contract with USAID, Contract Number _______________________ ("This Contract"), as a result of which the Contractor will have or require access to the USAID Global Acquisition & Assistance System (GLAAS). GLAAS is an integrated system, which currently incorporates the following key business functions of USAID: Procurement, Accounting and Document Generation. This agreement is hereby incorporated under Section M of "this contract."

The Parties to this Nondisclosure Agreement recognize that requirements of the performance of this Contract by the Contractor necessitate the Contractor's access to the GLAAS system.

1. Therefore the Parties agree as follows:

   a. USAID will make the GLAAS accessible to only the following employees of the Contractor:

Employee	**Position or Title**
_____________________________	_____________________________

   b. USAID will make the GLAAS accessible to only the following Subcontractors and to the following Subcontractor employees:

Subcontractor	**Employee**	**Position or Title**
_____________________	___________________________	__________________

2. The Contractor agrees that the Contractor, its employees, Subcontractors and Subcontractor employees working under this Contract, or having access to the GLAAS or information in the GLAAS, will not copy any information for the GLAAS except with the express authorized written approval of USAID. They will not publish or disclose to third parties, directly or indirectly, any procurement or source selection information, trade secrets, privileged information, confidential commercial or financial information, or any GLAAS software information. This includes documentation, acquired as a result of that access to information in the GLAAS, and that such information will not be disclosed to persons who work for or are in association with the Contractor, or its Subcontractors except those who have a need to know such information. Or those individuals who have already signed a personal Nondisclosure Agreement approved by USAID, before such employee(s) shall be provided access to the GLAAS. Such personal Non-Disclosure Agreement, at a minimum, must provide that such employee will not copy any information from GLAAS except with the express authorized written approval of USAID. Such employee agrees to comply with all provisions of law, including the Procurement Integrity Law 41 U.S.C. 423, and regulation with respect to procurement officials.

3. The Contractor further agrees that each of above-listed employees and each of above-listed Subcontractor employees, and all other employees and Subcontractor employees who have access to the GLAAS, will sign or will have signed a personal Non-Disclosure Agreement as provided in 2 above.

4. The Contractor acknowledges its understanding of the application of the Agency's Organizational Conflict of Interest Policy as stated in Contract Information Bulletin No.99-17 (located in Section K of USAID Acquisition Solicitations and Section M of USAID contracts) as well as the fact that procurement integrity provisions as stipulated in Section 27 of the OFPP Act, as amended by section 4304 of the National Defense Authorization Act remain in effect.

5. The Contractor agrees to indemnify and hold harmless the Government, its officers, and employees from and against all claims, demands, damages, liabilities, losses, suits and judgments which may be suffered by, accrue against, be charged to, or recoverable from the Government, its officers, and employees by reason of injury to third parties because of the contractors or its employees unauthorized disclosure to third parties of any trade secrets, privileged or confidential commercial or financial information, or procurement information the contractors or any of its employees acquire through access to GLAAS.

6. SURVIVAL. The Contractor agrees that the restrictions and obligations of Section 2 of this Non-Disclosure Agreement shall survive any expiration, termination or cancellation of this Contract or of this Non Disclosure Agreement, and shall continue to bind the Contractor and Contractor employees, the Subcontractors and Subcontractor employees; and their successors, heirs and assigns.

7. Term. The Parties agree that the term of this Nondisclosure Agreement shall be the same as this Contract, including the term of any modifications thereto.

8. Materiality. The Parties further agree that this Nondisclosure Agreement is a significant element of the Contractor's performance of this Contract, and any breach of this Nondisclosure Agreement shall constitute a material breach of this Contract.

Signed: ____ Date: ____________________
The Contractor

Signed: ____ Date: ____________________
Cognizant Contracting Officer
U.S. Agency for International Development

Signed: ____ Date: ____________________
GLAAS Executive Sponsor
U.S. Agency for International Development

PHOENIX ACCESS REQUEST ACKNOWLEDGEMENT

I acknowledge, as an Authorized Individual ("User") requiring access to the Phoenix financial system, that:

1. I am required to comply with USAID regulations, policies, procedures, and guidelines regarding the protection of USAID automated information systems from misuse, abuse, loss, or unauthorized access. I understand that any violation of those regulations may result in administrative action, civil or criminal prosecution, or termination of employment.
2. I must process only Unclassified information on systems designated for unclassified use, such as the Phoenix System.
3. I must protect my password and user ID. Should I suspect a compromise of my password or user ID, I must report suspected compromise to my supervisor and designated system administrator. I understand that my password will be changed immediately upon suspicion of compromise.
4. I must not share my user ID or password. I will not write down my password or user ID where others might easily find it. I can store my password or application users codes in an approved locking container or safe or otherwise protect its detection through the use of approved encryption technology.
5. I must not enter my password or application user ID in a file or record maintained in any automated system for the purpose of affecting an "autologin" feature for my convenience, unless the feature has been approved for use by the Information System Security Officer for USAID.
6. I must use/create a password consisting of a minimum of twelve characters that are not easily guessable or found in a standard dictionary. This must include a minimum of 1 Uppercase Alpha, 1 Lowercase alpha, 1 special and 1 numeric character. I am required to change my password at the interval prescribed for the system. I understand that USAID reserves the right to change my password or terminate my access at any time.
7. I must logoff or use a password protected screen saver at any time that I leave my terminal unattended. Should I expect to be away from my terminal for more than two hours, I will log off, even if a password protected screen saver is being used, to help minimize Agency software licensing costs.
8. I am required to immediately notify the system administrator for my system when there is a change in my employment status and/or when my access to the system is no longer required.
9. I may access only those applications and application subsystems for which access authorization by the system administrator has been granted and use government equipment only for approved purposes.
10. I am prohibited from using information acquired from access via a Federal computer system (including Phoenix) for personal gain, profit, or publication without the prior written approval of my supervisor.
11. I further understand that according to the *Phoenix* Financial System User Access Policies and Procedures, the following categories of personnel **may have access** to *Phoenix*: U.S. Direct Hires, FSN Direct Hires; U.S. PSCs; FSNs; WAEs; FSN PSCs; RSSAs and PASAs (U.S. Direct Hires from other Agencies); Detail-Ins from another Federal Agency, TAACs from another Federal Agency; and Population (TAACs) from PVOs; PMIs; Intern Investment Program and New Entry Professional Program. The following categories of personnel **require a waiver** in order to access *Phoenix:* AAAS Fellows; Population Fellows; Stars Fellows; Joint Career Corps; Inter-Agency Personnel Agreement; Institutional Contractors; Technical Advisors in Aids, Child Survival; Short-term Purchase Order employees and RSSAs and PASAs (Contractors from other Agencies).

USER STATEMENT: I certify that I have read and understand this Phoenix Access Request Acknowledgement. I also certify that I have already taken or intend to take the Phoenix Overview Training course.

_______________________ _______________________ __________ _________
User Name User Signature Office Symbol Date

SUPERVISOR STATEMENT: I certify that the above user falls under the category of (see item 11) ______________ and has a legitimate business need to use the Phoenix Financial System.

_______________________ _______________________ __________
Supervisor's Name Supervisor's Signature Date

WAIVER STATEMENT (IF REQUIRED): I certify that I have carefully weighed the risks of granting Phoenix access to the above named user and I have determined that this access is required to support critical operational needs of the Agency.

_______________________ _______________________ __________
Deputy Assistant Administrator (DAA) DAA Signature Date

Tiffany D. Adams_______________ _______________________ __________
Phoenix Information Systems Security Officer (ISSO) ISSO Signature Date

(rev. 1/19/2012)

This Page Intentionally Blank

Business Objects Enterprise Access Form

Instructions: *To request a Business Objects Enterprise, save a copy of this form to your local drive, then fill out the information below (press **Tab** to reach each field or **Shift + Tab** to go to a previous field). Send the completed form via e-mail to your supervisor for approval. Your supervisor must forward the form as an e-mail attachment to **CIO-HELPDESK-USAID**, with the stated approval in the body of the e-mail. The CIO Help Desk will forward your request to the appropriate Business Objects Enterprise point of contact (POC) for processing. (Note: Requests for access to folders with special access rights require additional approvals. If you have any questions, call the CIO Office at (202) 712-1234.*

REQUESTED BY:		
Date of Request:	**Name:**	
Position Title:	**Office Phone Number:**	**Network User ID:**
USAID Office:		**Country:**
Supervisor Name:	**Supervisor Position / Title:**	

Use the space below to list the name(s) of folder(s)/report(s) to which you require access.

ACCESS TO REPORTS REQUESTED:							
APC/GAO	**CRIS**	**EIMS**	**FS-AID**	**GLAAS**	**PHOENIX**	**WebTA**	**Other [Specify]**
☐	☐	☐	☐	☐OAA user ☐Non-OAA user	☐	☐	☐

Use the space below to specify access required.

LEVEL OF ACCESS REQUESTED:	
☐	STANDARD ACCESS
☐	OTHER. PLEASE SPECIFY