

Chapter 1 Concepts

OVERVIEW2
 AGPS Security2

Terminology3

Key Concepts.....4
 Overview4
 System4
 Screen.....4
 Record4
 Data Element4

Discussion ofTransactions5
 General Security5

OVERVIEW

AGPS Security The purposes of AGPS Security are:

- To provide a user specific access and function capability for AGPS
- To provide a user specific screen access
- To provide a user specific screen function authorization for AGPS screens
- To provide a user specific record access and maintenance authorization by agency

AGPS security is a four level security process providing access to the system, to screens, to records and to data elements. Security in AGPS may be tailored to the user's specific needs or may be general (security group) in nature.

Terminology

The following terms are used throughout this unit:

BAAT. This term is used to refer to the Access Authority Table. This table is used to identify users access to an agency's record(s) and maintenance authority. Additionally, this table is used to establish data element security by use of authorization codes when processing an agency's record(s) in a particular screen.

Data Element Security. This term is used to refer to maintenance capability for specific sensitive data elements.

FORT. This term is used to refer to the screen format table. This table is used to identify the program associated with a screen and those security groups identified in STAB that will be allowed access to a screen in AGPS.

Record Security. This term is used to refer to access to certain records and maintenance capability on those records.

Screen Security. This term is used to refer to access to certain screens and functions which can be performed using those screens.

Security Group. This is a term used to refer to a group security code established in the STAB Table to be assigned to multiple users with the same processing requirements in AGPS.

STAB. This is a term used to refer to the system access table in AGPS. All AGPS users must be identified in this table for access to AGPS.

System Security. This is a term used to refer to access to AGPS.

Key Concepts

Overview	AGPS has a four-level, top down security process providing access to the system, screens, records and data elements. It may be general in nature or tailored to a user's specific needs.
System	System security provides the user access to the system and establishes the functions allowed the user. This security is controlled by the USERID and password which are assigned and maintained in the STAB table.
Screen	Screen security provides the user access to a screen and controls the functions allowed to be performed with that screen by the user. This security is established using the FORT and STAB tables.
Record	Record security is controlled by the agency having the authority to maintain that record utilizing the BAAT (access authority) table. Access is controlled by agency number. Maintenance authority is established in the BAAT table by USERID.
Data Element	Data element security is to control the user's ability to update certain specific sensitive data elements within a record such as status. This security is established by the authorization code in the BAAT table.

Discussion of Transactions

General Security Visualize the system security as an upside down triangle.

<u>TYPE SECURITY</u>	<u>WHERE CONTROLLED</u>
SYSTEM	- STAB TABLES
SCREENS	- FORT & STAB TABLES
RECORDS	- BAAT TABLE (ORGAN & MAINT)
ELEMENTS	- BAAT TABLE (AUTH CODE)

SYSTEM (STAB)

The system security is controlled by the USERID and password. This is the USERID and password used on the AGPS screen for signing on to AGPS. This will merely give the person access to AGPS and not access to a screen, record or data element. The USERID and password are assigned and maintained in the STAB table.

SCREEN (FORT)

The screen security provides for access to and function of a screen. This security is established using the FORT and STAB tables. There are several issues involved here. First is access to the screen, that is can the USERID see the screen. Second is function, that is can the USERID perform an add, change, delete or inquire function.

RECORD (BAAT)

Now that security has been set up for the system and the screens, security must be established for the record. Security on the record is controlled by the agency having authority to maintain that record.

This is accomplished utilizing the BAAT (Access Authority) table. The BAAT table does two things. First, it controls access by agency number. The agency could be the requisitioning agency, purchasing agency, maintaining agency, etc. And second, it establishes the maintenance authority on the record as Y or N. In this manner a USERID may be able to inquire a record but not change it while another USERID may not be able to see the record.

An example for USERID and password FREDUSER:

USERID: FREDUSER

AUTHORIZATION CODE: 7777

AGENCY MAINTAIN

321XXX Y

This means that FREDUSER has access and maintenance ONLY for records where the agency number begins with 321 (321XXX). If BARNSELL is to have access without maintenance authority, then change the Y to and N under the maintain column.

DATA ELEMENT (BAAT)

This security is established by the authorization code on the BAAT (Access Authority) table. It allows the USERID and password the authority to change specific very sensitive data elements. An example is the authorization code on the VEND screen, authorization code on the PAPV screen, etc. A BAAT example of establishing an authorization code is as follows:

USERID: FREDUSER

AUTHORIZATION CODE: 1234

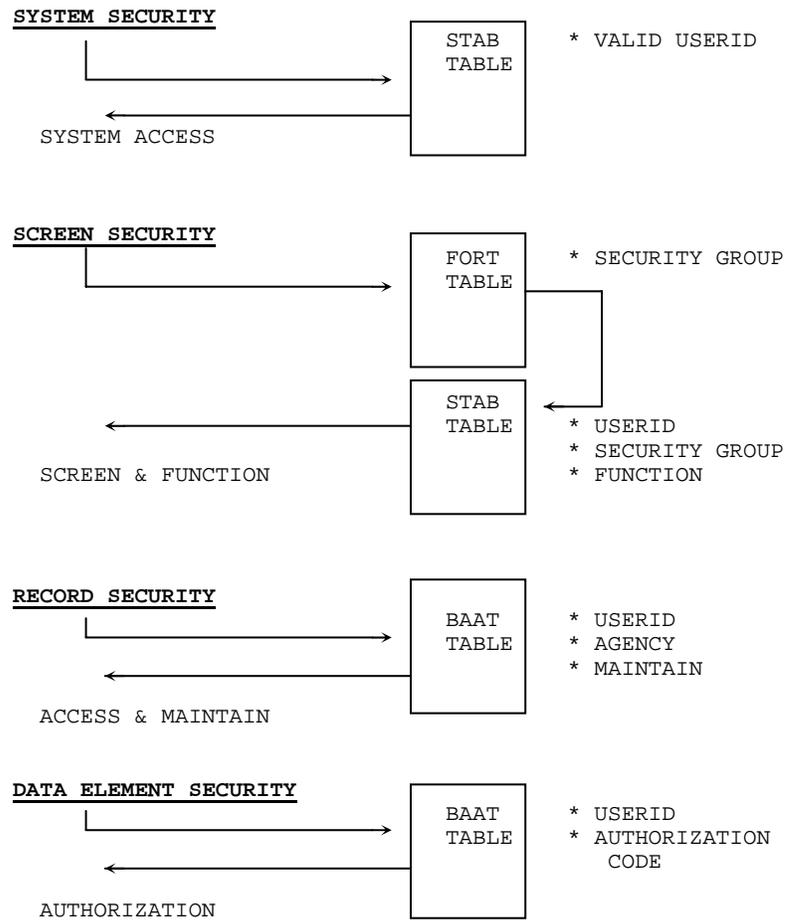
AGENCY MAINTAIN

321XXX Y

When the authorization code is blank, that particular USERID and password cannot change data elements where the screen requires an authorization code.

SUMMARY

Following is a graphic summary of the AGPS security process.



Whether a screen can perform a function is obviously controlled by the program behind the screen. If the program is not coded to perform a function, then the function cannot be performed. However, if the program is coded to perform a function, the function can be allowed for certain USERIDs and restricted for other USERIDs.