Table of Contents

Overview

Introduction   The Commonwealth Accounting and Reporting System (CARS) security
table determines user access to system features at the
- agency,
- user type, and
- user identification levels.

Users may or may not be permitted to inquire into or update system files and
tables.

Policy

**Security Table
Control**   The security table is controlled by the Department of Accounts (DOA). No
other user in the Commonwealth is granted access to this table.

CARS Security Officer

Introduction   Each agency is responsible for selecting **two key individuals** to be designated as CARS Security Officers (CSOs). These designations should be noted on the agency's *Authorized Signatories Form*. If the CSO changes, an updated *Authorized Signatories Form* should be submitted to DOA as soon as possible.

In addition, each agency head will serve as an ex-officio CARS Security Officer.

Duties   The duties of the CSO are as follows:

- control, within DOA constraints, an agency's access to CARS by its personnel,
- ensure adequate internal controls exist within that agency to prevent unauthorized access to online CARS data and datasets used to submit data into CARS,
- ensure that each logon ID (identification number) is assigned to an individual and not to an agency group or section, and
- serve as the liaison between DOA and all agency personnel who interact with CARS (including the Agency Access Coordinator), submit data to CARS, and hold an interest in CARS reports.

CARS Security Officer, Continued

Responsibilities   The CSO is responsible for the following, at a minimum:

- Maintenance of a comprehensive intra-agency system of internal control over both online and offline access to CARS tables, files, and datasets, within the constraints described in this section.

- Obtaining and filing completed Information Security Access Agreements from each CARS user with a logon ID beginning with "ACT." A completed (VITA_ISAA) Information Security Access Agreement must be obtained from the user prior to transmitting the (VITA03-001) *Logon ID Request - IBM Form* for an "ACT" logon ID. By signing the *Logon ID Request - IBM Form*, the CSO, is attesting to the completion of this requirement. These agreements are to be filed at the user agency and they must not be transmitted to DOA.

- Submitting timely security deletion requests for staff who should no longer have access to CARS. If a logon ID is going to be reassigned to another staff member, separate forms requesting the deletion of the current user and the addition of a new user should be submitted.

- Responding to the semi-annual security certification required by DOA. This includes reviewing the agency's access in its entirety and submitting required changes. This should be done periodically in addition to the semi-annual security certification.

- Receipt of CARS policies, procedures, and subsequent updates related to CARS security and dissemination to affected agency personnel.

CARS Security Officer, Continued

Scope of Authority

The CARS Security Officer may authorize access, within DOA constraints, to CARS for the agency number that corresponds to the *Authorized Signatories Form* designating CSO status. However, if a control agency's *Authorized Signatories Form* designates CSO status, that status is valid for that control agency as well as any "controlled" agencies. Control/controlled agency relationships are defined by the CARS D09 Agency Descriptor Table. See CAPP Topic No. 70225, *Descriptor Tables*.

Central agencies' [e.g., Department of Planning and Budget (DPB)] personnel may legitimately require access to agency data that exceeds the access allowed by the user type table (Exhibit 3). Any request for access beyond that reflected on the User Type Table should be made via a letter. The letter must include an itemized list of exceptions requested, with a justification for each exception, and be signed by the agency's CSO. Direct the letter to:

Assistant Director, DOA General Accounting
✉   gacct@doa.virginia.gov

A CSO cannot authorize security maintenance on their own logon ID(s). The alternate CSO must complete and submit the *CARS Security Maintenance Form*.

Establishing a CARS Logon ID

Introduction
The steps required to establish a logon ID in CARS are described in this subsection.

Security planning is crucial due to the number of parties involved and the specific constraints on user access to Virginia Information Technologies Agency's (VITA) computers and CARS files. Plan to take initial action at least one month in advance of anticipated system access. These procedures require involvement by agency personnel who are familiar with both CARS processing and agency internal controls. It requires coordinated action between:

- your agency's CARS Security Officer,
- your Agency Access Coordinator*,
- your agency's VITA Customer Liaison*,
- the DOA Database Administrator, and
- the DOA General Accounting Division.

To ensure prompt response to security access requests, follow these procedures closely and perform each step described in this topic in the sequence it is listed.

*To determine who these individuals are, contact VITA Customer Care at (866) 637-8482 or vccc@vita.virginia.gov.

Administrative Activities

1. Contact your agency's data processing department to determine if your agency has online access through existing agency hardware and communication lines to NG/VITA. If you do not have data processing staff, contact VITA Customer Care at (866) 637-8482 or vccc@vita.virginia.gov for assistance.

2. Complete and submit a new *Authorized Signatories Form* according to requirements in CAPP Manual Topic No. 20310, *Expenditures*.

   A new form is required if the logon ID is a user type 7 and that user is not currently listed on the form. A new form should also be submitted if a new CSO has been named.

3. Complete and submit *(VITA03-001) Logon ID Request - IBM Form*.

4. Complete and submit *CARS Security Table Maintenance Form*.

Logon ID Request – IBM Form (VITA03-001)

Introduction   The *(VITA03-001) Logon ID Request – IBM Form* must be accessed, completed, and submitted via VITA's website before an agency requests online access to CARS. The form must be signed by the Agency Access Coordinator and then processed by VITA (in the case of Agency Inquiry logon IDs) or by both DOA and VITA (in the case of Data Entry ACT logon IDs).

An agency should not submit the *CARS Security Table Maintenance Form* to DOA General Accounting until the *(VITA03-001) Logon ID Request - IBM Form* has been processed and the password has been changed for the logon ID.

Overview   Before establishing a new logon ID in CARS, submit the *(VITA03-001) Logon ID Request – IBM Form* to be processed. This form should be submitted by the Agency Access Coordinator.

All forms are submitted electronically to VITA. The form and instructions can be accessed at www.vita.virginia.gov/MISforms/forms/VITA03_001.cfm.

Logon ID   The logon ID is the "key" required by an individual to gain access to CARS. It also serves as the means by which VITA identifies which agency is to be billed for computer processing costs.

Data Entry vs. Inquiry Logon IDs   It is important to understand the difference between DOA and agency responsibility with respect to Data Entry and Inquiry Logon IDs.

Data Entry logon IDs are assigned by DOA and begin with the letters ACT. The Department of Accounts will pay for the computer processing costs accrued from the use of data entry logon IDs. DOA Agency Access Coordinators must establish, delete, and modify these logon IDs.

Data Entry logon IDs are limited to the following functions: financial data entry and updating the system tables.

Logon ID Request – IBM Form (VITA03-001), Continued

Inquiry logon IDs are assigned by the agency**.** The Agency Access Coordinator must establish, delete, and modify these logon IDs. These logon IDs begin with an abbreviation of the agency's name.

A user agency is billed by VITA for the computer processing costs accrued from the use of logon IDs that are assigned by the user agency. Inquiry logon IDs are allowed to perform all CARS functions, including financial data entry, table inquiries, updates and financial inquiry.

Passwords

Users must change their passwords promptly after new logon IDs have been established. To learn how to change a password, seek assistance from your Agency Access Coordinator.

Obtaining an Inquiry Logon ID and Password

To establish an **Inquiry** logon ID, the Agency Access Coordinator must access and complete the *(VITA03-001) Logon ID Request - IBM Form* on VITA's website*.* This form is completed online and submitted electronically. Detailed instructions on how to complete the form can be found on VITA's website at www.vita.virginia.gov.

VITA will establish the logon ID in COMPLETE (the software that allows access to CARS online screens) with access suspended and will notify the Agency Access Coordinator once completed.

NOTE: The Agency Access Coordinator must then un-suspend the logon ID, and the user must change the password, before the CARS Security Officer can submit the *CARS Security Table Maintenance Form* to DOA.

Obtaining a Data Entry Logon ID and Password

To establish a **Data Entry** logon ID that begins with ACT, the Agency Access Coordinator must complete the *(VITA03-001) Logon ID Request - IBM Form* and submit it to DOA Database Administration via email to wayne.gabbert@doa.virginia.gov.

Continued on next page

Logon ID Request – IBM Form (VITA03-001), Continued

The Logon ID is established by DOA Database Administration. The CSO will be provided with the Logon ID and password that is established. When the user of the Data Entry Logon ID logs on to CARS for the first time and enters the password provided, they will then be informed the password has expired and will be required to enter their own unique password.

Agency or VITA staff can assist with password issues for **Inquiry** logon IDs (logon IDs that do not begin with ACT).

VITA staff or DOA Database Administration staff can assist with password issues for **Data Entry** logon IDs that begin with ACT.

CARS Security Table Maintenance Form

Introduction   To gain access to CARS, a *CARS Security Table Maintenance Form* must be submitted by the agency's CARS Security Officer (CSO). All forms are submitted electronically to DOA. The form can be accessed at http://www.doa.virginia.gov/General_DOA/DOA_Forms_Alpha.cfm. A sample of this form is provided in Exhibit 1.

An email will be automatically generated to send the form to DOA once the form is completed and the CSO selects "Submit to DOA". The e-mail with the attached form must be from the same CSO whose name is typed on the form.

Overview   A *CARS Security Table Maintenance Form* is completed for each user identification number (user ID) to be established in the CARS Security Table. For the CARS Security Table, the user identification number is the same as the ACF2 logon ID.

All coding on the *CARS Security Table Maintenance Form* must be reviewed carefully before submission to DOA. DOA will not correct unknown errors or omissions on the form.

The following sections provide details for each of the major components of the security table. The major components include:

- Function
- User Information
- Access Agencies
- Table Maintenance Functions
- Financial Data Functions
- Other Functions

Continued on next page

CARS Security Table Maintenance Form, Continued

Function   The function codes used to update the security table are as follows:

Code	Function
A	**A**dd a new user ID to the table.
C	**C**hange name or user access (including deleting a specific function) in the table. When deleting a specific function or making a change such as a name change, type a message that identifies the change in the body of the e-mail that transmits the *CARS Security Table Maintenance Form.* Note: For any changes to an existing user ID, only the data to be changed should be entered on the *CARS Security Table Maintenance Form.*
D	**D**elete user ID from the table.

CARS Security Table Maintenance Form, Continued

User Identification Elements

The four elements which identify each user on both the *CARS Security Table Maintenance Forms* and the security table are the
- user identification number (user ID),
- user agency,
- user type, and
- user name.

Part	Function
User ID	The User ID is a seven position field and is the logon ID previously established by submitting the *(VITA03-001) Logon ID Request - IBM Form*. ACT logon IDs will be provided to the CARS Security Officer by DOA.
User Agency	Three-position numeric field that identifies the State agency with which the user is associated. The agency code must be on the D09 (Agency) Descriptor Table.
User Type	One-position field that identifies and classifies the type of user. Each user type is designed for specific access and capabilities within CARS. These capabilities are determined by several factors. Each user type is restricted to certain input values for the various security table functions. Exhibit 3 outlines the capabilities for those users whose Security Table data entry indicator is **Update**. The CSO must limit requests for type **7** access to those individuals who appear on the agency's *Authorized Signatories Form*.

CARS Security Table Maintenance Form, Continued

User Type, continued	User Type values are:
	4 = Central Agency Inquiry
	5 = Agency Inquiry
	6 = Agency Data Entry
	7 = Agency Approval
User Name	Thirty-position field that contains the user's legal name.

Access Agencies   The Access Agencies component of the security table and form allows a maximum of 40 state agencies to be specified per user ID. For state agencies specified in this area, the user may inquire into or update financial information, based on user type. All agencies entered in this area must be on the D09 (agency) descriptor table. The CSO signing and e-mailing the *CARS Security Table Maintenance Form* to DOA must be listed as CSO for each agency listed in the Access Agencies section of the form or the Control Agency of those listed.

If the user is to be allowed access to all state agencies, ALL should be entered in the first agency field. **ALL** may be used for User Type **4** only.

Table Maintenance Functions   The Table Maintenance Functions component of the security table and form allows a user to inquire into or update system tables. There are 44 table maintenance functions that may be independently specified for each user ID. Exhibit 2, Section 3 provides a detailed description of specific system functions, by user type, that are controlled by the table maintenance functions. Exhibit 4 also provides a key for agency access to the Descriptor Tables.

The valid values for these functions are:

Update
Inquiry
Blank (No Access)

oContinued on next page

CARS Security Table Maintenance Form, Continued

Financial Data Functions   The Financial Data Functions component of the security table and form allows a user to inquire into or update system tables. There are 4 financial data functions that may be independently specified for each user ID.

The four functions are:

- Data entry
- Error correction
- Financial inquiry
- 1099 File inquiry

Exhibit 2, Section 4 provides a detailed description of specific system functions, by user type, that are controlled by the Financial Data Functions.

Data Entry   The Data Entry function provides the user with the capability to enter or view financial transactions through the standard input screens.

Valid values for the **data entry** indicator are:

Update
Inquiry
Blank (No Access)

Error Correction   The Error Correction function allows the user to enter error corrections or view error transactions. **Only DOA personnel can enter error corrections through the error correction screens**.

Valid values for the **error correction** indicator are:

Update [DOA personnel only]
Inquiry
Blank (No Access)

Continued on next page

CARS Security Table Maintenance Form, Continued

Financial Inquiry

The Financial Inquiry function allows the user to access the financial inquiry screens.

Valid values for the **financial inquiry** indicator are:

Yes
Blank (No Access)

1099 File Inquiry

The 1099 File Inquiry function allows the user to access the 1099 adjustment screens. The Yes value allows a user to view or update.

Valid values for the **1099 file inquiry** indicator are:

Yes (view or update)
Blank (No Access)

Other Functions

The Other Functions component of the security table and form allows a user to inquire into or update system tables. There are 6 other functions that may be independently specified for each user ID.

The six functions are:
• report request
• news screen
• required edit option
• forced entry
• reverse code
• modifier

Exhibit 2, Section 5 provides a detailed description of specific system functions, by user type, that are controlled by the other functions.

Report Request

The Report Request function allows the user to request standard reports. **Only DOA personnel can request reports through the report request screens**.

Valid values for the **report request** indicator are:

Yes [DOA personnel only]
Blank (No Access)

CARS Security Table Maintenance Form, Continued

News Screen   The News Screen function allows the user to view or update the news broadcast screen with user defined messages. **Only DOA personnel can update the News Screen, all other users can view the News Screen as they logon to CARS.**

Valid values for the **news screen** indicator are:

Yes [DOA personnel only]
No Access—View only

Required Edit Option   The Required Edit Option function specifies the lowest level of edit option that can be used by the user ID when financial transactions are entered through the on-line data entry screens.

As batches are created and transactions are input into CARS, the operator must select from the following values for required edit option (See CAPP Topic No. 70230, *Data Entry*):

Blank	Access Not Allowed
A	Simple data entry (not used at this time)
B	Data-related editing

If the Required Edit Option is:	then the user . . .
No Access	Cannot enter financial transactions.
A	Not currently used
B	May specify Edit Option **B** on input.

Forced Entry   Not available in CARS at this time.

CARS Security Table Maintenance Form, Continued

Reverse Code   The Reverse Code function allows the user to input data into the reverse code field on detail transactions. **Only DOA personnel can utilize the Reverse Code function.**

Yes [DOA personnel only]
Blank (No Access)

Modifier   Not available in CARS at this time.

Completing and Submitting the CARS Security Table Maintenance Form

After accessing the *CARS Security Table Maintenance Form* at http://www.doa.virginia.gov/General_DOA/DOA_Forms_Alpha.cfm, enter the appropriate information using the instructions on DOA's website or in Exhibit 5.

Review the form carefully prior to submission as DOA staff will not correct unknown errors or omissions on the form. Submissions must be received from an agency CSO. The e-mail, with the form attached, must be sent by the CSO whose name is typed on the form. When appropriate, click the "Submit to DOA" button at the top of the form. An e-mail from the CSO will be generated with DOA's General Accounting e-mail address. Click send and the e-mail will be sent to DOA General Accounting staff at gacct@doa.virginia.gov. If additional information is needed, DOA General Accounting staff will contact the CSO.

After all processing is completed by DOA staff, a signed form will be routed back to the submitting CSO via e-mail. Upon receipt of the signed form from DOA, review it to make sure all changes made to the security table are as the agency intended for the user. Completed *CARS Security Table Maintenance Forms* should be kept on file at the requesting agency for review. DOA recommends storing copies of authorized forms in a secure location.

Questions regarding this process can be directed to gacct@doa.virginia.gov.

Dataset Access

Transfer File Security

Agencies that transfer files from their internal financial system to CARS must take appropriate steps to ensure all necessary security measures are in place for individuals that have access to enter and approve financial transactions into agency based systems that interface to CARS. Additionally, these measures should also include IT staff that have access to files transferred to CARS. Agencies must have documented internal control policies and procedures in place to ensure security access granted is necessary and appropriate and is authorized by appropriate agency management. These policies must include a periodic review to ensure security access remains current and appropriate. All individuals who have authority to authorize and approve financial transactions contained in an agency dataset to be processed in CARS should appear on the agency's *Authorized Signatories Form.*

DOA Control Restrictions

Enforcement

Exhibit 2 provides a summary of the access allowed to each function by user type. DOA will audit each *CARS Security Table Maintenance Form* by this summary.

1. DOA will not correct any errors or omissions on the form.
2. All CARS edit criteria and agency restrictions on Security Table access must be met.
3. For any changes to a given user ID in the security table, only the data to be changed should be entered on the *CARS Security Table Maintenance Form*.
4. Central Agencies (e.g., Department of Planning and Budget) personnel may legitimately require access to agency data to an extent not allowed by the *CARS Security Table Maintenance Form*. Any request for access beyond the form restrictions should be made via email to the Assistant Director, General Accounting at gacct@doa.virginia.gov. The request should include an itemized list of exceptions requested, with a justification for each exception and be sent by the agency's CARS Security Officer.
5. Users with Type 7 access must be on the agency's Authorized Signatories Form.

The Department of Accounts strictly enforces its published restrictions on access to CARS functions through Security Table updates. However, each online agency has considerable latitude, within DOA constraints, to enter, manipulate, and purge its own data. Each agency head must ensure that an effective, agency-based, internal control system exists to protect agency data.

Internal Controls

The control of an agency's access to CARS is vital. The CARS Security Officer is responsible for a comprehensive system of internal control over both online and offline access to CARS tables and files. This access control is vital to ensure the integrity of accounting transactions submitted to CARS. The internal control system must be documented sufficiently to allow its examination by the Auditor of Public Accounts. DOA is not responsible for the existence, design, or function of such internal control systems.

Records Retention

CARS Security Table Maintenance Forms must be retained for three (3) years or until audited by the Auditor of Public Accounts, whichever is longer.

Subject Cross References

CAPP Topic No. 20310—*Expenditures*
CAPP Topic No. 70225—*Descriptor Tables*
CAPP Topic No. 70230—*Data Entry*

Contacts

Director, DOA General Accounting
☎ (804) 225-2376
FAX (804) 225-4250
✉ gacct@doa.virginia.gov

DOA Database Administration
☎ (804) 371-0199
FAX (804) 371-8587

Exhibit 1: CARS Security Table Maintenance Form

Commonwealth of Virginia
CARS Security Table Maintenance

I hereby request that you update the CARS Security Table as specified below. In conjunction with this request, I certify that this action conforms to all requirements for the security table maintenance specified in the Commonwealth Accounting Policies and Procedures Manual. Further, I certify that this agency maintains a system of internal control over on-line access to CARS adequate to prevent unauthorized access to or changes in the data contained therein, and that the use of this form constitutes an integral part of the internal control system.

By typing my name below and submitting this form to DOA, I am certifying that I am the CARS Security Officer of the agency and authorize the update to the CARS Security Table as specified on this form.

Name: _____ , CARS Security Officer
Agency: _____
Phone Number: _____ **Extension:** _____
E-mail Address: _____ **Date Submitted:** _____

Function:

User Information

User ID: _____ **User Type:** _____
First Name: _____ **Last Name:** _____
Agency: _____

Access Agencies

Table Maintenance Functions

Function	01	No Access	ORG Level 1	10	No Access	Task	19	No Access	CDS	35	No Access
Subfunction	02	No Access	ORG Level 2	11	No Access	Phase/Year	20	No Access	Revenue Class	36	No Access
Program	03	No Access	ORG Level 3	12	No Access	FIPS	21	No Access	Project Type	37	No Access
Service Area	04	No Access	ORG Level 4	13	No Access	PSD	22	No Access	Subsidiary Account	38	No Access
Element	05	No Access	GLA	14	No Access	Bank Code	23	No Access	Federal Catalog	39	No Access
Fund	06	No Access	Major Object	15	No Access	Payment Type	24	No Access	Batch Type	40	No Access
Fund Detail	07	No Access	Subobject	16	No Access	Pre-Audit	30	No Access	Register Type	41	No Access
Secretarial	08	No Access	Revenue Source	17	No Access	GAAP Fund	31	No Access	Error Code	51	No Access
Agency	09	No Access	Project	18	No Access	GAAP Subfund	32	No Access	Error Element	52	No Access
						CAFR Conversion	33	No Access	VA Power Acct. No.	53	No Access
Transaction Code		No Access	Cost Code		No Access	Vendor Edit		No Access	Project Control		No Access
Security		No Access	System Mgmt		No Access						

Financial Data Functions

Data Entry		No Access	Error Correction		No Access	Financial Inquiry		No Access	1099 File Inquiry		No Access

Other Functions

Report Request		No Access	News Screen		No Access	Required Edit Option		No Access		
Forced Entry		No Access	Reverse Code		No Access	Modifier		No Access		

Exhibit 2: Security Table Maintenance Summary

The restrictions over a user type's access to CARS functions are summarized below. The section numbers are for reference when looking at Exhibit 1, *CARS Security Table Maintenance Form.*

	User Type			
Item	**4**	**5**	**6**	**7**
Section 1:				
Name, CSO	R	R	R	R
Agency Number and Name	R	R	R	R
Phone Number	R	R	R	R
CSO e-mail address	R	R	R	R
Date (automatically populates)	R	R	R	R
Section 2:				
Function	A, C or D	A, C or D	A, C or D	A, C or D
User ID	R (1)	R (2)	R (2)	R (2)
User Agency	R (5)	R	R	R
User Type	4	5	6	7
User Name	R	R	R	R
Access Agencies	(3)	(4)	(4)	(4)

Legend:
   A = **A**dd, C = **C**hange, D = **D**elete, R = **R**equired

Notes:
  (1)   User ID prefix must be ACT if Agency = 997; otherwise prefix must not = ACT
  (2)   User ID prefix must not = ACT if any indicators are set as I or Y
  (3)   Can equal "ALL" or from 1 to 40 individual agencies from the D09 table
  (4)   Must = User Agency. If User Agency is a control agency, access agencies may include controlled agencies.
  (5)   Must = 122, 133, or 997

Section 3:				
Function	I	I	I	I
Subfunction	I	I	I	I
Program	I	I	I	I
Service Area	I	I	I	I
Element	I	I	I	I
Fund	I	I	I	I

Exhibit 2: Security Table Maintenance Summary, Continued

	User Type			
Item	**4**	**5**	**6**	**7**
Fund Detail	I	I	I	I
Secretarial	I	I	I	I
Agency	I	I	I	I
Org Level 1	I	I	U, I	I
Org Level 2	I	I	U, I	I
Org Level 3	I	I	U, I	I
Org Level 4	I	I	U, I	I
GLA	I	I	I	I
Major Object	I	I	I	I
Subobject	I	I	I	I
Revenue Source	I	I	I	I
Project	I	I	U, I	I
Task	I	I	U, I	I
Phase / Year	I	I	U, I	I
FIPS	I	I	I	I
PSD (Political Subdivision)	I	I	I	I
Bank Code	I	I	I	I
Payment Type	*	*	*	*
Pre-Audit				
GAAP Fund	*	*	*	*
GAAP Subfund	*	*	*	*
CAFR Conversion	*	*	*	*
CDS				
Revenue Class	I	I	I	I
Project Type	I	I	I	I
Subsidiary Acct	I	I	I	I
Federal Catalog	I	I	I	I
Batch Type	I	I	I	I
Register Type	I	I	I	I
Error Code	I	I	I	I
Error Element				
VA Power Acct No	*	*	*	*
Transaction Code	I	I	I	I
Cost Code	I	I	U, I	I
Vendor Edit	I	I	U, I	I
Project Control	I	I	I	I
Security				
System Management	I			

Exhibit 2: Security Table Maintenance Summary, Continued

	User Type			
Item	**4**	**5**	**6**	**7**
Section 4:				
Data Entry	I	I	U	U
Error Correction	I	I	I	I
Financial Inquiry	Y	Y	Y	Y
1099 File Inquiry	Y	Y	Y	Y
Section 5:				
Report Request				
News Screen				
Required Edit Option			B	
Forced Entry				
Reverse Code				
Modifier	*	*	*	*

Legend:
I = Inquiry
U = Update
Y = Yes (inquiry allowed)
Blank = Not allowed
B = Required Edit Option Indicator
* = Function not available in CARS at this time
Any element may be left blank; blank allows no access. Items above with no indicator must be blank.

Exhibit 3: Access Allowed by User Type

The Security Table's data entry indicator has valid values of Update, Inquiry, and Blank (no access). The value Update grants a range of capabilities to the operator that depends on that operator's user type, established elsewhere in the operator's Security Table record.

The relationship between a data entry indicator of Update and the operator's access to CARS capabilities appears in the following table.

System Capabilities		User Types			
		4	**5**	**6**	**7**
• View batch headers		*	*	Y	Y
• View transactions		*	*	Y	Y
• Add batches		*	*	Y	N
• Change batch headers		*	*	Y	N
• Delete batches		*	*	Y	Y
• Change batch status:					
From	**To**				
Agency Hold	Agency Release	*	*	N	Y
Agency Release	Agency Hold	*	*	N	Y
Agency Release	Pre-Audit Hold	*	*	N	N
Agency Release	Pre-Audit Release	*	*	N	N
Pre-Audit Hold	Pre-Audit Release	*	*	N	N
Pre-Audit Hold	Agency Hold	*	*	N	N
• Add transactions		*	*	Y	N
• Change transactions		*	*	Y	N
• Delete transactions		*	*	Y	N
• Change Vendor Payment Status		*	*	N	N

Legend:
Y = Yes
N = No

* Valid values for the data entry indicator for User Types 4 and 5 are confined to Inquiry or No Access.

Exhibit 4: Descriptor Table—Key for Agency Access to Tables

TABLE NUMBER	TABLE TITLE	AGENCY INQUIRY	UPDATE	PRINTOUT OF TABLE AVAILABLE (2)
01	Function	Yes	No	No
02	Sub-Function	Yes	No	No
03	Program	Yes	No(1)	No
04	Service Area	Yes	No(1)	No
05	Element	Yes	No	No
06	Fund	Yes	No	No
07	Fund Detail	Yes	No	Yes
08	Secretarial Area	Yes	No	No
09	Agency	Yes	No	No
10	Organizational Level 1	Yes	Yes	Yes
11	Organizational Level 2	Yes	Yes	Yes
12	Organizational Level 3	Yes	Yes	Yes
13	Organizational Level 4	Yes	Yes	Yes
14	GLA	Yes	No	No
15	Major Object	Yes	No(1)	No
16	Subobject	Yes	No(1)	No
17	Revenue Source	Yes	No	No
18	Project	Yes	Yes	Yes
19	Task	Yes	Yes	Yes
20	Phase/Year	Yes	Yes	Yes
21	FIPS	Yes	No	No
22	PSD	Yes	No	Yes

Exhibit 4: Descriptor Table—Key for Agency Access to Tables, Continued

TABLE NUMBER	TABLE TITLE	AGENCY INQUIRY	UPDATE	PRINTOUT OF TABLE AVAILABLE (2)
23	Bank Code	Yes	No	No
24	Payment Type	No	No	No
30	Pre-Audit	No	No	No
31	GAAP Fund	No	No	No
32	GAAP Sub-fund	No	No	No
33	CAFR Conversion	No	No	No
35	CDS	No	No	No
36	Revenue Class	Yes	No	No
37	Project Type	Yes	No	No
38	Subsidiary Account	Yes	No	No
39	Federal Catalog	Yes	No	No
40	Batch Type	Yes	No	No
41	Register Type	Yes	No	No
51	Error Code	Yes	No	No
52	Error Element	No	No	No
53	VA Power Acct. No.	No	No	No
	Transaction Code	Yes	No	No
	Cost Code	Yes	Yes	Yes
	Vendor Edit	Yes	Yes	No
	Project Control	Yes	No	No
	Security	No	No	No
	System Management	No	No	No

Exhibit 4: Descriptor Table—Key for Agency Access to Tables, Continued

Notes:

(1) The Department of Planning and Budget (DPB) authorizes establishment of these specific codes, maintenance of related tables and use of these codes by agencies. **Direct all inquiries to DPB**.

(2) Printouts for the indicated CARS tables are available through the following reports.

Report Name	Report Number
Descriptor Table Report	ACTR0900 (see Note B below)
Cost Code Table Report	ACTR0920 (see Note A below)
Project Control Table Report	ACTR0930 (see Note A below)
Vendor Edit Table Report	ACTR0940 (see Note A below)

(A) **These reports are issued upon request only**. To request these reports, send an e-mail to gacct@doa.virginia.gov.

(B) **Descriptor Table Reports, ACTR0900, is available for individual tables**. To request a report, send an e-mail to gacct@doa.virginia.gov. The table number desired must be included in the e-mail. For example, an agency wanting a printout of project codes would request table D18. (See preceding list for descriptor table numbers.)

Exhibit 5: Completing the Electronic CARS Security Table Maintenance Form

Department of Accounts
CARS Security Maintenance Form Instructions

Open the form on DOA's website in Adobe Reader. Enable JavaScript if not enabled. Complete the name, agency, phone number, extension (if applicable) and e-mail address of the CARS Security Officer (CSO). Date Submitted will be auto-populated once the user submits to DOA.

Select Add, Change or Delete for the *Function*. For changes, complete all of the fields through *Access Agencies* and only the additional or changed fields in the *Table Maintenance*, *Financial Data* or *Other Functions* areas.

Complete the *User Information* area with the correct data for the CARS user to whom the User ID will be assigned. All User Information fields are required to be completed.

Complete the *Access Agencies* area with at least one agency selected from the first drop-down box.

Complete the *Table Maintenance Functions*, *Financial Data Functions* and *Other Functions* areas for the User Type designated. Refer to CAPP Topic 70220 for the functions affiliated with a specific User Type. Based on the User Type indicated, drop-down boxes may reflect I for Inquiry, U for Update, Y for Yes, or blank if no access is allowed. If the User ID is to be deleted, do not complete any of the following functions.

Please do not key data in the *Department of Accounts Use Only* area.

After all information has been entered, the CSO should 1) print the form for agency records by clicking **Print Form** and 2) submit the form by clicking the **Submit to DOA** button. If a required field is not completed when the Submit button is clicked, an error message(s) will appear identifying the field(s) that needs data or correction. Correct the field and click Submit again. If all required fields are completed, the CARS Security Maintenance Form will be attached to an e-mail. Send the email to DOA (gacct@doa.virginia.gov). CARS Security Maintenance Forms processed by DOA staff will be returned via e-mail to the CSO who sent the request. Returned forms should be kept for agency records.