eMARS Security and Workflow Plan

INTRODUCTION

One of the primary requirements of any financial system is to maintain data integrity. A key component of maintaining data integrity is the successful implementation of security administration. System security is a critical aspect in the implementation of eMARS.

The purpose of this paper is to describe the approach for eMARS application security and approval workflow and to describe how the setup will occur. Information from this paper will be used to prepare the Central and Agency Security Administrators Guide.

The approach of security is to provide a high degree of accountability, integrity, and confidence within eMARS without making it impossible to use or administer. Users must be able to use the system, and administrators must be confident that the users will be able to perform only the necessary actions within the scope of their job functions.

Document approval processing is a system of routing documents through Advantage Workflow to users or groups of users for review/approval prior to "finalizing" the document. Workflow provides the technical means of electronically routing document data to the next resource.

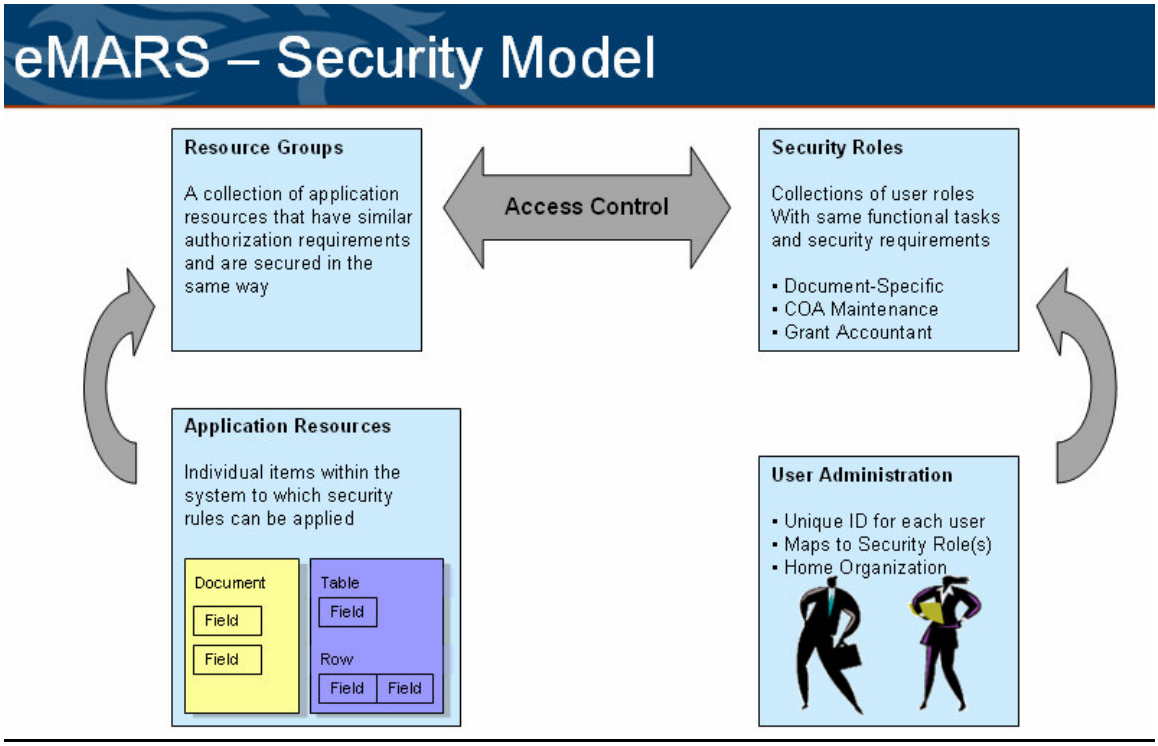
Approval processing provides a powerful, automated means of human authorization of document data prior to finalization.

The Commonwealth's goal is to develop a security and workflow model that meets the following:

- Model will be in place when system "goes live", ensuring a secure environment
- Model ensures appropriate internal controls/segregation of duties are accounted for
- Model will be flexible enough to account for changes in business processes (i.e. Re-organizations or policy/procedure changes)
- Model can be easily maintained and administered

ADVANTAGE 3 SECURITY MODEL

The figure below is an illustration of the various security model components in Advantage 3 and their relationships. The numbers correspond to the typical order in which you define these components.



1. Resource Group – A collection of application resources that have similar authorization requirements and are secured in the same way.

2. Application Resources – Items within Advantage 3 (such as tables, documents, inquiries and HTML pages) to which security rules are applied. If needed, the row filtering function can be activated at this level to prevent users from seeing rows in tables that have secured fields. Also, user interface (UI) field security is activated at this level to prevent users from seeing or accessing data on a page that has secured fields.

3. Security Role – Groups of users with the same functional tasks and security requirements. They are defined for groups of users and not for individual users. Individual users are given their security by being assigned to one or more Security Roles.
4. Access Control – Controls which Security Roles have access to which Resource Groups and the extent of that access. It defines the actions (i.e. open, save, submit, etc…) that users within a given Security Role can perform on these resources. It controls the approval levels for the combination of Security Role and Resource Group. Additionally, it manages the Foreign Organization definitions associated with Security Roles/Resource Group combinations and provides control over the activation of field security.

5. User ID – A unique identifier assigned to each user that enables the user to log on to the application and links the user to one or more Security Roles.

6. Secured Fields – If security requirements include restrictions at the field level, the central security administrator will define which fields on tables and documents are secure, set up the security rules for these fields, associate these fields with Application Resources, and activate the field security function at the Access Control level.

Application Resources: Data Object (Internal) and Page (External) Resources

Application Resources are categorized one of four ways: document, reference table, query, or page. Resources defined as documents, reference tables or queries must be defined on the Application Resources table; otherwise, no one will be able to access these items. Page resources are an exception to this rule. They must only be defined on the Application Resources table if they are to be secured. The central security administrator will add all resources to the Application Resources table and associate each one with a Resource Group (which is similar to a security group in Advantage 2). **Note: Application Resources can be associated with only one Resource Group**.

In "baseline" Advantage, out of the box, no *pages* are defined as application resources. What does this mean? What is a page? A page is simply an HTML view of a data object. For example, there is an HTML page code called FUND (where all Advantage 3 fund codes are established) and this would be an "external" resource if defined on the Application Resource table. The name of the table in the Advantage 3 database (where the data is stored) is R_FUND and this is an "internal" resource.

Because no pages are defined on the Application Resources table (out of the box) a user's security is controlled entirely by the internal (database) resources, not by the HTML page codes. This means that a user inherits the access rights to "view everything and do nothing". Why? When you access a page code from within the application, security verifies that you have access to that "page". Pages can only be secured if they are defined on the Application Resources table. Since they are not set up on this table you will be able to open the page (i.e. FUND page).

Only when you try to "commit" something to the internal database table (R_FUND in this case) security will verify if you are authorized to perform the action.

In the proposed Commonwealth model we will define every HTML *page* code as an application resource and assign it to its own Resource Group. The name of the Resource Group will be the HTML page code. This will make the Resource Group easier to identify when establishing the Access Control records (assigning it to Security Roles).

Security Analysis Tools

CGI-AMS is working on a new page-level security model to be delivered as the "baseline" approach in future releases. Esbjorn Larsen from CGI-AMS was here the first week of June 2005 to demonstrate this model to the Commonwealth. We decided on our security model at the conclusion of this "training".

We will use page-level security to allow easy management of table dependencies (essentially eliminating the dependencies). By setting up all pages as application resources a user will not have access to view a page unless specifically granted that access. The user will no longer have the "view everything do nothing security". As mentioned previously each page will be assigned to a resource group with the name of the group being the HTML page code. Since security is controlled at the resource group (and not the application resource) this will make it easier for us to identify exactly what a resource group encompasses.

We were provided with Excel spreadsheet tools that will do the following: load all HTML "pages" to the Application Resources Table and load all Resource Groups. The "internal" resources will be combined in two Resource Groups: INT_QRY and INT_TBL.

The spreadsheet tools will also facilitate in the creation of Security Roles and Access Control Records. Analysis and implementation will be managed using the Security Analysis and XML Generator spreadsheets. The XML files will be loaded using SysManUtil.

Home and Foreign Organization Security

Users in Advantage 3 are assigned (on the SCUSER table) to a Home Organization. All organizational elements (Branch, Cabinet, Dept, Division…..Unit) are available to choose as the Home Organization. The appropriate Department code will be populated for each user. Also, each user will be assigned a Bureau of CPTL. The Department and Bureau codes must be valid codes (correctly set up on their respective tables).

All Unit codes will roll up to the CPTL Bureau except for those identified as "pro card" units. There will be a unique Unit code established for each pro card site. These Unit codes will roll up to the PCRD Bureau. In order to restrict a user's access below department (for non pro-card tables/documents) the appropriate fields on SCUSER, besides Dept and Bureau, must be populated (i.e. Division, Group, Section or District).

Access Control records are established by the central security administrator and can be defined by Foreign Org security (instead of Home Org security). When selected, Foreign Org table entries will be added to identify the organizations the Security Role/Resource Group will have access to.

Foreign Org security can be a bit misleading, though, because a user not only has access to the records indicated on the Foreign Org table; he also has access to his Home Organization (from the SCUSER table). If we only identified a Dept on the SCUSER table for a user this could cause a security problem. All pro card tables/documents will be secured by department **and** unit code. The pro card roles will be controlled by "Foreign Org" security (dept and specific unit). However, it is important to ensure a pro card admin cannot access pro card data for other units in his Dept. To prevent this we are going to assign/rollup all "Procard" units to a Bureau of PCRD.

This means our security roles will be controlled by Foreign Org Security, Home Org Security or by NONE (statewide access).

Row Filtering, Secured Fields and User Interface (UI) Security

Row Filtering

This functionality is "turned on" at the application resource level. When this flag is selected, Advantage checks the user's security setup when that user tries to view records from this table. If any of the organizational or other secured fields in the row are not authorized, the user is not allowed to view the record.

Using this function may impact the performance of Advantage because implementing it is processing-intensive. Specifically, when a user accesses a page displaying a resource for which row filtering has been enabled, Advantage performs the following checks for each row to be displayed:

- Organizational Security Type check – Do the user's Home and Foreign Organization field values meet the requirements for this security check?
- Field Security check – Does this resource have secured field(s) associated with it? If so, has field security for this Resource Group been activated and do the field values meet the requirements for this security check?

Based on these checks, Advantage either displays the row to the user or filters it out so that the user does not see it.

Field-Level Security

In addition to defining security on resources such as documents and tables, the central security administrator can control the authority users have for table resources or documents based on the values of individual fields present on the table or document. This type of security neither prevents users from seeing the secured fields nor from updating their values. Rather, it secures the entire record based on the secured fields' values in addition to the organizational security authority check. In order to prevent users from seeing table rows in which a secured field appears, the row filtering functionality (as described above) must be implemented for the table after the secured fields are defined.

User Interface (UI) Security

User Interface (UI) Security is a flexible security feature that can be configured to *protect* or *protect and mask* fields in Advantage that the Commonwealth deems sensitive and confidential. The UI Security table can be set up to protect individual fields from changes, as well as to control the display of text input fields. Display of these fields can be set up in one of three ways:

- Fully Masked and Protected – The field is displayed showing as many asterisks as the size of the field.
- Partially Masked and Protected – Specific number of characters (as defined by Commonwealth) at the end of the field are displayed, with the preceding characters masked and displayed as asterisks.
- Protected only – The contents of the field are not masked, but the field is still protected from changes

ADVANTAGE 3 WORKFLOW and APPROVALS

A document may require up to 15 levels of approval. For each approval level you can define rules for requiring that approval level, establish a routing destination and a routing sequence, and indicate whether an automatic E-mail notification should be sent to the user or group where the work unit is being routed.

Some of the common terms of Advantage Workflow are explained below:

- Work Unit – Indicates the item for which workflow is being performed. In Advantage the work unit is a document
- Approval Rule – Determines which, if any, approval levels are required for a work unit, and if so, defines the approval routing properties (i.e. assignee, routing sequence, and so forth)
- Approval Condition – Used to construct approval rules. Each condition evaluates up to five approval fields and values to construct a condition for requiring approvals
- Approval Fields – Individual value containers used to construct approval conditions. They can be defined for document headers and document line fields
- Approval Comments – Descriptions that can be attached to approval routings to inform the recipient of the work item of the purpose of the routing
- Approval Hierarchy – Used to define the hierarchy in which the document approvals are performed

Approval assignments can be routed to Approval Roles or users. Each approval level can be assigned to only one Approval Role or one user. Each approval level can have a maximum of 5 or conditions, and each OR condition can have a maximum of 5 AND conditions. **Note: AND conditions may not contain fields from more than one component unless one of the component types is the document header.**

Each approval level is assigned to an ordinal number (routing sequence) that specifies when the approval level assignment should be displayed in the assignee's worklist. Approval levels with a lower ordinal number will be assigned earlier than levels with higher ordinal numbers. Approval levels with the same ordinal number will appear in the assignee's worklist at the same time.

To enable approval processing for a document code, the following three fields on the DCTRL table (General Options subsection) must be set as follows:

- Set the **Submit Phase** field to *Pending*
- Change the **Workflow Process Indicator** to *Internal*
- Leave the **Workflow Asynchronous Processing** flag unchecked. This allows a document to be automatically processed to *Final* once the approval processing has been completed

WORKLISTS AND PENDING PHASE

When a document is ready for approvals it will be submitted for Approval Processing, moving the document from *Draft* to the *Pending* phase. Documents are assigned a Pending phase during the entire Approval Process, until the document is ultimately approved or rejected by all applicable Approval Levels. **Note: When a document is in a PENDING phase it is "read-only". The document can only be APPROVED or REJECTED. If any changes need to be made to the document it must be rejected back to the DRAFT phase. Then, after the corrections have been made, submitted back through Workflow (PENDING phase).**

Documents may not be approved from the Document Catalog. The only way to approve a document is by accessing it from a Worklist. Each user is assigned a "personal" Worklist. Users may also belong to one or more Approval Roles. Each Approval Role has its own Worklist.

If the assignee on an Approval Rule is an individual the document will be sent to their personal Worklist and only that user can approve/reject the document. If the assignee is an Approval Role any member of that role (with that approval level specified in one of their security roles) can approve the document through the Approval Role's Worklist. When a document is sent to an Approval Role one member of the Role must select the document and click "Take Task". This moves the document from the "Role" worklist to their "personal" worklist. **Note: All documents must be approved from your personal worklist**.

Additionally, one or all members of an Approval Role can be set up as a Manager for that role. When you are viewing an Approval Role worklist and you are a Manager for that role, then you see a **Manager Worklist** link at the bottom of the worklist page. This link enables you to access the manager worklist for that workflow role. This page is similar in nature to the regular worklist page. All worklist actions are supported and the interface is consistent with the regular worklist pages. In addition the role Manager can:

- View the items currently assigned to all role members.
- Return items from a user's worklist to the role worklist for reassignment.
- Directly apply an approval action (i.e. Reject or Approve) to an item in a user's worklist.

Approval Rules

Each document, when submitted for Workflow/Approval Processing, is assigned to one (and only one) Approval Rule. The Approval Rule is selected based on the document code and the document's organizational values. The applicable Approval Rule for a document code is the one that most specifically matches the document's organizational values.

Each Approval Rule can require up to 15 levels of approval, and each level consists of up to five approval conditions joined by logical OR's. If any of the approval level's conditions evaluate to "true", then that approval level is required. Each OR condition can have a maximum of 5 AND conditions.

Security Roles and Approval Roles

Users can belong to multiple Approval Roles. They do not have to be granted the approval *authority* that corresponds to the approval role. A user may wish to view the documents in Workflow, but, does not have to actually Approve/Reject the document. Users are assigned approval level authorities based on the security roles they belong to. The Agency Security Officers will need to make sure that "approvers" in their agency are not only assigned to the correct Approval Roles, but, are also granted the appropriate security roles that correspond to the Approval Roles.

Agency versus Central Approvals

With assistance from the Agency Implementation Team and the Central Security Team, each Agency Security Officer will be responsible for determining the required approval levels for each document in addition to assigning their users to the Approval Roles (assigned to each level). Some documents will not require "central" approval while other documents (such as the CR document) will also be approved centrally.

The eMARS Implementation Team is tasked with identifying all "central" approval levels and it will be the Central Security Administrator's responsibility to ensure these approval levels are added to each necessary Approval Rule table entry. For example, all Approval Rule table entries for the CR (cash receipt) document must have the approval levels defined for the State Treasurer's Office so that they are the "final" approval for all CR documents.

Detailed Security Approach

Application Resources and Resource Groups

We have chosen to implement our security model based on "page" security instead of "table" security. This means that every HTML page in the application must be defined as a resource on the Application Resources table. Each of these resources (defined as a page) will be assigned to its own resource group, and the name of the resource group will be the HTML page code. This will make it easier to establish security on the **Access Control** table for the Security Role – Resource Group combinations.

CGI-AMS has provided the Commonwealth with the spreadsheet tools to load the entries for the Application Resources and the Resource Group tables. As with all the security tools, the analysis of the data will be on the Excel spreadsheet, itself. Based on the analysis of the spreadsheet, we will generate XML files to mass-insert into Advantage (using the SysManUtil functionality).

Next, we need to identify the HTML pages we will not be using (i.e. unused budget structures, HR pages, etc…). On the **Application Page Registration** (APGS) table we will uncheck the *Searchable* flag for these resources. The flag indicates whether the page can be searched from the Page Search Window. If it is not checked the page cannot be accessed in this window. **Note: The Security Team will work with each of the functional team leads to identify the pages the Commonwealth will not use at implementation.**

At this point the Application Resource and Resource Group tables have been established and we are ready to identify our security roles. The CGI-AMS provided spreadsheet tool will facilitate the creation of the security roles.

Security Roles

Each of the HTML page codes (Resource Groups) are identified on the spreadsheet in a separate row. Then, each Security Role is entered in a different column. Under each security Role we'll enter a "U" (update) or "R" (read) for each of the page codes the Security Role should have access to. The role will only have Update or Read access to the pages that are selected. **Note: The Security Team will work with each of the functional team leads to identify the security roles to be established in each functional area.**

Our security roles will be set up based on functional area. For example, we will establish procurement roles, fixed asset roles, payable/disbursement roles, grants/project roles, etc…Then, users are granted the applicable roles, as needed. This will be easier to manage instead of creating "generic" roles that encompass multiple functional areas.

We will utilize the "ANY" security role where applicable. This is a security role that is set up in the application (Security Role and Access Control tables) but it is implicitly assigned to all users, meaning it will not appear as a role granted to a user (on the Security Roles/Users link page). This role will consist of **view-only access** to tables and queries that do not contain data that is "sensitive" in nature. For example, the following types of tables may be added to this role: Object, Fund, Department, Revenue Source, etc…This will make the creation and maintenance of the security roles more manageable.

Users can be assigned an unlimited number of security roles. So, when a user's access requirements change we can adjust their security simply by adding or taking away security roles (which will not affect other users). The other option would be to change their existing role (which could inadvertently impact other users belonging to that role) or create a new security role, which is time-consuming (and will require a "bounce" of the application before it can be used).

The name of the security role is only **8** characters in length and this is how we're proposing to name them. The first three characters will be the dept (i.e. 750) or cabinet (i.e. C39) code. Statewide roles (those controlled by home organizational security) will be assigned **ALL**; characters 4 – 6 will be a "description" (i.e. PO, FA, COA, CR); character 7 will be "access" (R, U or A…for Read, Update or Approve); and character 8 will be home organizational security type (H, F or N…for Home, Foreign or None).

For example, a user at the Dept of Parks may have the following security roles:

- ALLMA_UH Create/Update Master Agreements for home organization
- 670CR_AF Create/Update/Approve Cash Receipts for home + foreign orgs
- ALLJV_UH Create/Update Journal Voucher documents for home org
- C50PAYRF Read/View Payables documents for cabinet 50 (foreign org)

Once we've identified our security roles on the "analysis" spreadsheet we can use the XML generator to create the XML files containing both the Security Roles and the Access Control table entries. Then, we'll use SysManUtil to mass-insert the table entries (XML files) to the application.

The *Organizational Security Indicator* on the Access Control table for the agency security roles will be set to either *Foreign* or *Home*. Many users will require access to only their own department so their roles would be set up with Home Org security. Others, needing access to multiple departments will have their roles defined at Foreign Org security. This is done on **Foreign Organization** table entries that are associated with the Security Role – Resource Group combination.

"External" versus "Internal" Security

With the "page" security model a user will not have access to an HTML page unless specifically granted access in a security profile. This security only controls access to the page, itself. It does not control access to the "internal" tables updated by reference tables or by documents.

For example, in order to process a GAX document the user must have "update" access to the following "internal" application resources: **R_AP_DISB_RQST**, **R_AP_CHK_RECON**, **R_CBAL**, **R_FBAL**, etc…Access to the GAX page (to create, validate and submit the document) does not automatically grant a user access to update these table entries when validating or submitting the document. The user must be granted access to these internal resources.

All "internal" application resources are grouped together in two resource groups: **INT_QRY** for system queries and **INT_TBL** for reference tables. Users are granted "read" access to the internal queries and "update" access to the internal tables. This is the key feature of the page security model: **A user is granted access to update the internal application resources, but, can only do so through the HTML page codes he is granted access to**. For example, a user will be granted "update" access to the internal fixed asset tables (by granting him "update" access to the INT_TBL resource group); however, he is not assigned a security role that gives him access to any of the fixed asset *pages* (documents or tables). Therefore, he does not really have access to update these internal resources.

Document Security: Header and Posting Line

All documents are secured organizationally at the document header, meaning a user can only open documents (from the Document Catalog, Worklist or application links) for his Home Organization and for Foreign Organization table entries for that document page. While organizational security is enforced at the header level it is not "automatically" checked at the posting line level.

As previously mentioned, when a document is processed several "internal" resources (reference tables, journals, etc…) are updated, and the user must have UPDATE access to these resources. In our initial model we chose to group these tables in the INT_TBL resource group and the user will have UPDATE access to the organizations specified in his security roles.

There's one major drawback, however, to this security model that is different than what we have in Advantage 2 today. When you grant a user UPDATE access to the INT_TBL resource group he will have that access for all documents he has access to process (validate, submit, approve, etc…). In Advantage 2 you can be granted access to process documents for one or more agencies and, then, be granted access to different agencies on another document. For example, a user in Revenue may have access to process CR documents for five agencies, but, can only prepare other MARS documents for Revenue only. This cannot be done without modifications to our security model.

There are really two ways to "get around" this problem in Advantage 3 without changing our model. First, we could activate "component-level security" for documents, which involves Versata changes (1-2 lines for each document) and may adversely impact system performance. On the other hand we could assign a second user ID to an individual, if necessary, so the user can perform their job duties. In our "Revenue" scenario above a user can be granted access (under one user ID) to submit/approve CR documents for multiple agencies. That is all the access that one ID would have. Any other Advantage 3 functions would have to be performed using another user ID (that only had access to submit/approve documents for Revenue only).

According to CGI-AMS no other client site has activated component-level security for all their documents. Component-level security is typically implemented on a document by document basis. Implementing component-level security across all documents could have an impact on system performance; therefore, we will test this functionality to determine the performance impacts.

I believe component-level security would be the easiest to manage on an ongoing basis. Under this model users will be granted full update access (all organizations) to the INT_TBL resource group. With component-level security activated on the Accounting line component, the same "security check" performed on the document header (DOC_HDR) component will also be checked on each accounting line (DOC_ACTG_LN).

Now, the Application Resources, Resource Groups, Access Control entries and Security Roles have been established and loaded to the Advantage application (using the security analysis tools and spreadsheets). Before we add users to the application and assign them security roles there are a few table settings and configurations we need to finalize.

Row Filtering – Application Resource Table

First, we need to determine what tables we want to activate "row filtering" for. This functionality is "turned on" at the application resource level. When this flag is selected, Advantage checks the user's security setup when that user tries to view records from this table. If any of the organizational or other secured fields in the row are not authorized, the user is not allowed to view the record.

Using this function may impact the performance of Advantage because implementing it is processing-intensive. Nevertheless, there are tables/queries where we'll want to utilize this functionality. We should not use this functionality as a "convenience" tool; we should not use it if the only reason is to prevent a user from having to do a "search" to find what he's looking for. For tables with "sensitive" information we will certainly utilize row filtering.

Note: The Security Team will work with each of the functional teams to identify the tables the Commonwealth will want to implement row-filtering on.

Field Security and User Interface Security

We must identify the application resources (and field values on them) where we'll want to use the field security and/or user interface security functionality. Field security secures the entire record based on the secured fields' values in addition to the organizational security authority check. User Interface Security is a flexible security feature that can be configured to *protect* or *protect and mask* fields in Advantage that the Commonwealth deems sensitive and confidential (such as TIN and bank account number).

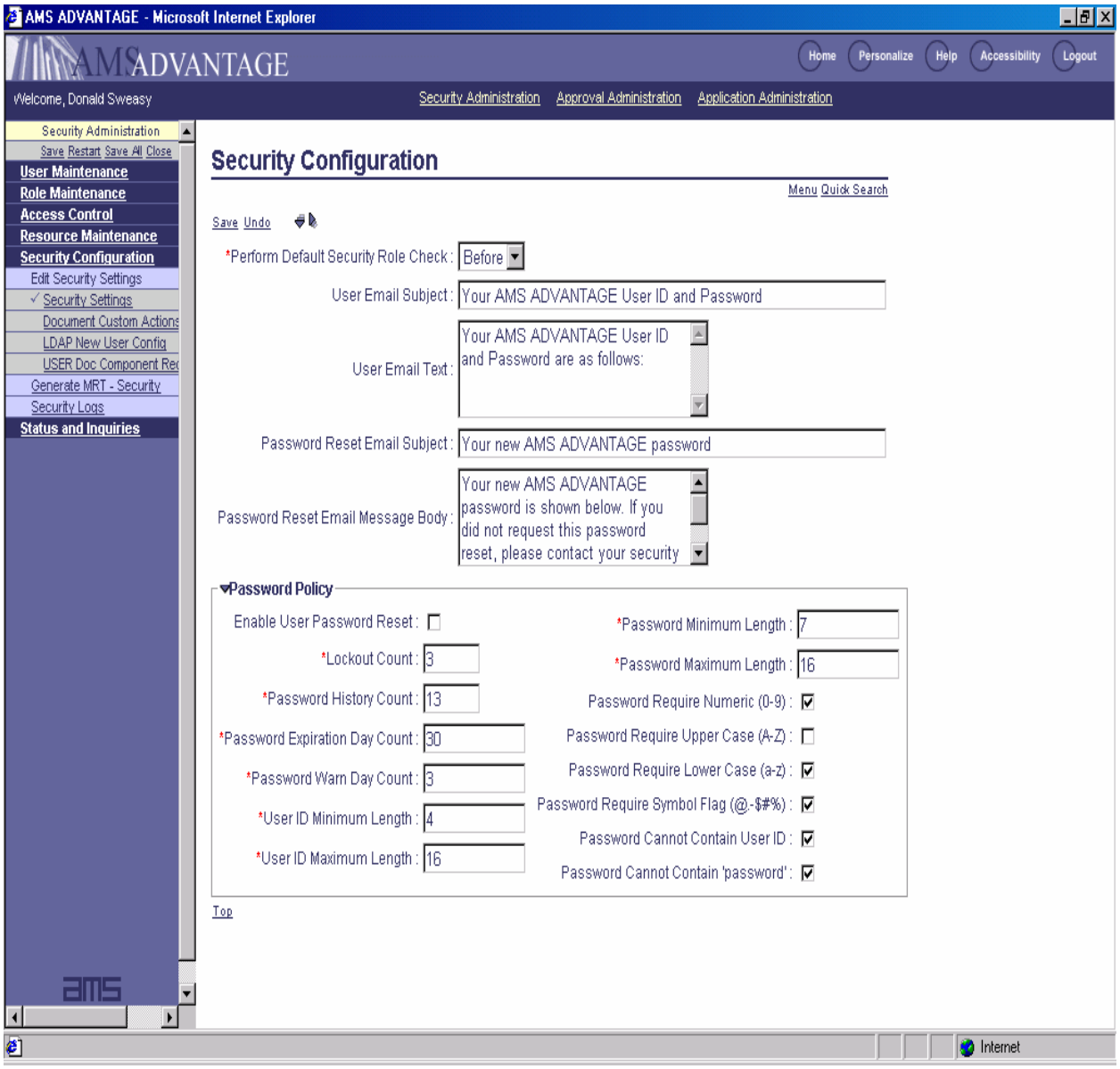
Some likely candidates are the VCUST table (TIN, bank account number, credit card number) and the GAX document (Disbursement Priority and Single Payment Flag).

Note: The Security Team will work with each of the functional teams to identify the resources the Commonwealth will want to implement field security and user interface security on.

Security Configuration Table

We need to determine the security requirements for user ID's, passwords, etc…on the Security Configuration table. First, we need to identify the naming convention to be used for user ID's. This will be left up to each department/cabinet. Some may want to use their RACF user ID (for those users who also use RACF) while others may want to use something like their NT user name or a first initial + last name. We will not require RACF user ID's to be established if the user is not going to access RACF with it.

After identifying the naming convention we must identify requirements for user ID's and passwords. Our recommended settings are shown below:



Detailed Workflow Approach

All documents will be submitted for approval processing so no document should reach the FINAL phase when submitted. To prevent this from happening there will be one "default" rule for each document code used in the application.

On the Approval Setup table the organizational values for each of these rules will be wildcard values (????), from Government Branch – Unit. The document will have only one assignee and it will be an Approval Role titled "**Do Not Approve**". The central security administrators will be assigned to this approval role and an E-mail will be sent alerting them when documents are sent to this role worklist. This approval rule should never be assigned to a document. It is meant to serve as a "catch-all role" to keep a document from posting to FINAL when submitted. The central security administrator will be responsible for taking action on items in this worklist.

One example of when this could be used is when a new department is added. Assume department 700 is added to the application and all system tables are updated correctly except for the Approval Setup table. When a document is submitted and there is not an approval rule set up for department 700 (or one for its cabinet rollup) the "default" approval rule will be applied to the document. Based on the settings on the Approval Setup table an E-mail will be sent to the central security administrators (assigned to the "Do Not Approve" approval role) and they'll be responsible for making the necessary corrections.

We'll set up a "default" rule for each department. In some cases (particularly with smaller departments) this will be the only rule defined. For some larger departments who may establish rules below the department level (i.e. Division, Group, Unit, etc…) this could serve as a "catch-all" rule for their department. This will also ensure that, at implementation, all submitted documents will (at least) be assigned an approval rule in that department.

Identify Approval Conditions

An approval condition is defined for a document code and can have maximum of 5 sub-conditions. Each of these 5 sub-conditions are logically linked together with AND statements. Each sub-condition consists of a document code field, an operator (=, >, <, In List, Is Null, etc…), and a literal value. A document code field must be defined before it can be used in a sub-condition. These approval condition definitions are used when defining the rule(s) for an approval level on the Approval Setup page.

Note: During our testing we determined that the "right-hand"/evaluation side of the condition cannot contain a blank space. For example, we initially established our Cited Authority codes with a "blank space" (i.e. FAP 111-09-00-04). We established the following approval condition: CITED_AUTH = FAP 111-09-00-04. This condition was not activated on the approval setup table. We changed the cited authority on the Cited Authority table to read FAP111-09-00-04 and set up a similar approval condition as above (without the blank space). This time, the approval condition was activated.

The Security Team will be responsible for working with the agency Security Officers to determine what these conditions will be.

Define Approval Fields

Once the approval conditions have been identified the fields affected will need to be set up on the Approval Fields table. For example, we will use the Cited Authority field as a conditional field in approval processing. So, the CITED_AUTH field code must be set up on this table. Likewise, if a rule is set based upon a particular fund coded on a document then the FUND_CD field must be defined as an approval field.

The Security Team will be responsible for populating the Approval Fields table and will work with the agency Security Officers to identify these fields.

Define Approval Conditions

The conditions defined earlier must now be set up on the Approval Conditions table. For example, one approval condition table entry may be set up for the following on the PO document: Cited Authority = FAP111-09-00-04 **and** Total Dollar Amount >= $1,000.00.

Define Approval Roles

Documents can be sent to individual users or to a group of users (Approval Roles). For all approval rule entries the document will be sent to an approval role (for all approval levels). This will make the maintenance of approval processing much easier. Unless there is a change in business processes there will never be a need to make a change to the “main” workflow table, the Approval Setup table. The only maintenance will be adding/removing users from the list of Approval Roles they belong to.

Any user in an Approval Role can be made a “Manager” of that role.

There is a new baseline enhancement that will be introduced with Advantage 3.6 that allows a system administrator to select the approval roles assigned to one user and copy any number of them to another user. Thus, when a user retires, transfers, etc…and a new user takes his place he may need the exact same security as the other user. There is functionality, now, that allows the system administrator to copy both the security and approval roles from one user to another.

Define Approval Rules

Each Approval Rule is set up on the Approval Setup table. This table is the driving force behind Advantage Workflow. On this table, you set under which conditions each document code for a specific organization (cabinet, department, division, unit…etc) is routed for approval. Up to fifteen levels of approval can be specified and an approval role will be assigned for each level.

As mentioned previously there will be “default” Approval Rules for each document code (system-wide) and a “default” Approval Rule for each document code in each department. Depending on the particular document this one rule may be the only one the department wishes to create for that document code.

Note: The Security Team will work with the Agency Implementation Team and each of the Agency Security Officers to identify the most effective set of Approval Rules for each department.

Because departments operate differently from one another it's not feasible to set up a "generic" set of rules that each will have to adhere to. Some cabinets push more work out to their "field" offices and may require more rules while some cabinets have central processing shops that do much of their work. These cabinets may require fewer approval rules.

On approval rules for payment documents the submitter of the document will not be allowed to apply an approval on the document. There is a "restricted approver" checkbox on each approval rule and we'll restrict the submitter from approving any payment documents. This will ensure a user cannot submit a payment to Workflow and approve the same transaction. For other documents it will be up to the agency security officers to determine if they want this restriction on other documents, as well.

The Security Team will need to work with each of the functional teams to identify any "central" approval conditions that will need to be defined and set up for each Approval Rule table entry. For example, all CR documents must have an approval condition set up on the Approval Setup table so Treasury will be the final approver for all CR documents. Without a doubt, we anticipate the Procurement Team will have more "central" conditions defined than any other functional area. We will reserve certain approval levels (depending on particular document code) for these central approvals.

Because of the number of potential Approval Rule table entries (possibly 10,000 +) we'll need to develop a spreadsheet that can be loaded to the Advantage 3 tables. The Security Team will be responsible for developing this spreadsheet.

Assign Approval Authority to Users

In order to approve a document two things must happen: first, a document must be in your worklist (sent to an Approval Role). Second, you must have a Security Role that grants you the authority to apply the level of approval required on the document (approval level shows up on Worklist). For security roles with approval authorities assigned we plan on assigning all "agency" levels of approval to that role. Then, we'll use the Approval Rules to determine when that user can actually apply that approval. This will reduce the number of security roles we have to establish and will make ongoing maintenance (post-implementation) easier to manage.

When a user's approval authorities change for a document he will only need to be added to/removed from the applicable Approval Roles. We won't have to make any changes to his Security Roles.

We're exploring the option of allowing the agency security officers to add/remove users from Approval Roles assigned to their organization. They will not be allowed to alter the Approval Setup table or assign their users to any "central" approval roles. They will only be allowed to add/remove users in their own agency from approval roles in their own agency.

Project Timeline

August 2005

- Finalize and sign off on Security/Workflow Model
- Test security and workflow functionality in 3.6.1a and 3.6.1b
  - Log issues in Incident database
- Begin assigning Resource Groups to **ANY** Security Role
- Start to identify Application Resources (Pages) we don't plan on using
- Develop and Process test scripts for security and workflow
  - Organizational security (Cab, Dept, Div, Bureau and Unit)
  - ANY Security Role
  - Row Filtering, Secured Fields and Foreign Org access
  - Approval Rules: Cab, Dept, Div, Bureau and Unit level rules

September 2005

- Initial meeting with all Agency Security/Workflow Officers
  - Introduce Security and Workflow "model"
  - Gather feedback and input
  - Show examples in application
  - Begin training (TBD) for Agency Security Officers
- Test security and workflow functionality in 3.6.2
  - No "new" security/workflow functionality in this drop
- Begin developing Security Roles
- Develop spreadsheet(s) that Agency Security Officers will use for setup:
  - Approval Fields
  - Approval Conditions
  - Approval Comments
  - Approval Roles
  - Approval Rules

October 2005

- Assist Agency Security Officers with Approval/Workflow setup
- Identify all "central" Approval conditions (approval levels)
- Row Filtering: Identify Application Resources to "filter"
- Finalize list of Security Roles

November 2005

- Test security and workflow functionality in 3.6.3
  - Pro Card modifications are in this drop
  - User Interface (UI) Field Security is in this drop

- Provide Agency Security Officers with spreadsheets to establish their Workflow setup (i.e. Approval Fields, Conditions, Roles, Comments and Rules)

December 2005

- Begin populating Security and Workflow setup tables with spreadsheets sent in from agencies

- Test agency approval conditions and approval rules. Central Security Team will develop test scripts to test a variety of approval conditions and rules

- Define uses for field security and UI field security

January 2006

- Finnish collecting security and workflow spreadsheets from agencies

- Grant agency security officers (and others, if needed) access to the "testing" region where we loaded their security and workflow spreadsheets

- Provide assistance to agency security officers in their "testing"

February 2006

- Begin loading "finalized" security and workflow settings in a "production-like" region
  - APGS Entries
  - Application Resources and Resource Groups
  - Setup for UI Field Security, "Row" field Security and Row filtering
  - Security Roles
  - Approval Fields, Approval Conditions and Approval Comments
  - Approval Roles and Approval Rules

March 2006

- Work with "central" agencies (i.e. Finance, Treasury, GOPM, etc… to develop security roles specific to their central organization

- Finalize agency approval and workflow setup in "production-like" region

April 2006

- Agencies will submit spreadsheets with user information/security roles
- Production-Like region should now be loaded with all security and workflow tables (including security roles, approval roles and approval rules)
- Central security team and agency security officers will spend several weeks "banging away" at application…looking for any security holes, defects, problems, etc…with the current setup
  - Main focus will be on tables and documents that will be used on May 15

May 2006

- Load security and workflow setup tables from "production-like" region to the production application
- Load users to production application and sent out logon requirements (for certain users)
- Application available for use on May 15 (certain functions)
- Continue testing in "pre-production" application
- Verify security/workflow is working properly in production environment

June 2006

- Focus on production environment
- Modify any security/workflow configuration settings in production environment
- Activate all "active" users

July 2006

- Full Implementation July 1
- Support Agency Security Officers
- Post-Implementation Updates
  - Add/Edit Security Roles
  - Add/Edit Approval Setup Table entries