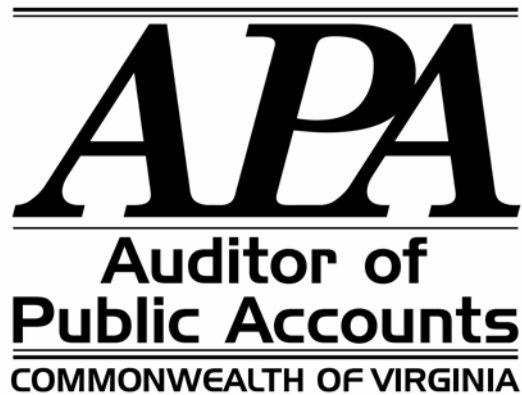


DEPARTMENT OF GENERAL SERVICES
eVA SECURITY REVIEW

JUNE 2005



EXECUTIVE SUMMARY

We have completed a review of eVA security management, as it existed in January 2005. This review primarily addresses central security administration activities performed by General Services. We will address agency security administration activities during their individual audits.

Overall, we found that General Services has established strong policies and procedures, but there are areas for improvement over eVA security administration. We recommend that General Services:

- develop exception-based queries to analyze user access on a regular basis. General Services should communicate exceptions and their resolution to agency security officers;
- make monitoring tools available to agencies on-line so agencies can more efficiently and effectively meet their monitoring responsibilities;
- periodically assess agency security practices and their compliance with the eVA security manual; and
- provide formal security training to security officers on a regular basis and develop a formal strategy to increase security delegation to agencies.

General Services has stated their ultimate goal is to delegate advanced security administration functions to the agencies that have sufficient, qualified resources to fulfill these responsibilities. By improving each of these areas, General Services will move closer to their overall goal of delegating advanced security functions while ensuring the integrity of eVA.

-TABLE OF CONTENTS-

	<u>Pages</u>
EXECUTIVE SUMMARY	
INTRODUCTION	1
BACKGROUND INFORMATION	1- 3
RECOMMENDATIONS AND FINDINGS	3- 7
INDEPENDENT AUDITOR’S REPORT	8- 9
DEPARTMENT OF GENERAL SERVICES’ RESPONSE	10-11

INTRODUCTION

The Department of General Services (General Services) launched eVA as the Commonwealth of Virginia's electronic procurement system in March 2001. eVA is an internet-based, purchasing service solution provided by CGI-AMS and administered by General Services. It allows users to initiate purchases and obtain appropriate approvals through automated workflows and vendors to access the Commonwealth's procurement opportunities through a single location.

Our office completed two interim reports addressing areas needing attention for successful implementation of the eVA solution. These reports, entitled "Commonwealth's Electronic Procurement System, eVA," dated May 31, 2002 and December 6, 2002, outline the original design, functionality, funding, and usage, as well as address the Commonwealth's procurement policies and operating environment.

Since March 2001, eVA has processed over 640,000 orders totaling \$5.8 billion. As of May 2005, 171 state agencies and 475 localities have implemented eVA and almost 27,700 vendors have registered. eVA also has over 9,000 individual buyer users.

As an internet-based application, all users access eVA from any internet connection. That means buyers can initiate purchases from their office, their homes, their local library, and any other place where they have access to the internet. Vendors can access eVA from the same locations. They simply direct their web browser to the eVA portal, www.eva.virginia.gov; type in their user ID and password; and they have access to all of their authorized privileges.

Internet-based applications create flexibility, but also create inherent security risks. Users can access eVA from anywhere, so traditional controls such as individual agency firewalls and network authentication processes do not protect access. Anyone can attempt to access eVA and with the right combination of privileges, users who fraudulently access eVA, could attempt to make fraudulent purchases. This intensifies the need for strong controls.

Given the size of the user population, the number of transactions, the dollars involved, and the unique risks presented by an application accessed through the internet, we have completed a review of eVA security management, as it existed in January 2005. We took the security measures in place at that time and performed our work. We updated any findings or other information through the date of this report. This review primarily addresses central security administration activities performed by General Services. We will address agency security administration activities during their individual audits.

BACKGROUND INFORMATION

User Account Administration and Approval Workflow

User ID's control the type of access users have within eVA. The security officer assigns each user ID access to specific functionalities, such as the eMall, and associates specific rights and privileges that identify what a user can do with their assigned functionality. For example, their rights and privileges in the eMall would define what they could buy, how they could pay for it, and how much they could spend. Once established, eVA also allows users to self-administer their shopping access, meaning they can request changes to these access rights and privileges on-line.

Various approvals, as defined by each agency, lay on top of the user's rights and privileges through a tool known as workflow. eVA allows the agency to design and associate approvals based on a transaction's attributes, such as dollar amount, cost code, commodity code, or even the type of access change request.

Thus, the nature of the transaction will define its approval workflow. It is the agency's responsibility to ensure their approval workflows provide appropriate controls over the procurement process. General Services provides guidance to the agencies in the design of the approval workflows, as discussed in more detail below.

eVA Security Management

eVA, as an internet-based purchasing solution provided by an external organization, makes security management a multi-organization effort. It relies on activities performed by CGI-AMS, General Services, and individual agencies.

CGI-AMS

As the service provider, CGI-AMS maintains control and responsibility for providing system accessibility that does not compromise data integrity. CGI-AMS has contracted with various companies for delivery of specific components of eVA, including secure hosting, networking, eMall functions, document management and data analysis tools. CGI-AMS and its subcontractors monitor eVA for technical performance and hardware security management. General Services requires CGI-AMS to have an independent audit of their responsible areas and therefore, our audit did not include a review of CGI-AMS or their subcontractors.

General Services

General Services retains responsibility for the next layer of security on behalf of the entire Commonwealth, known as eVA Global Security. The global security officer administers the overall configuration and security of eVA applications and has the following responsibilities:

- reviews, verifies, and establishes agency security officers;
- periodically reviews and assesses agency security practices and their compliance with the eVA Security Manual;
- facilitates and monitors agency compliance with applicable federal and state statutes and policies; and
- coordinates security awareness training for agency security officers.

General Services has designated internal procurement staff as agency account executives to assist agencies in their use of eVA and advise them on the procurement process and policies and the Virginia Public Procurement Act. Account executives act as liaisons between global security and the agency to communicate issues as they arise and distribute guidance as necessary. General Services has assigned each agency a specific account executive, providing them a consistent, single point of contact.

Individual Agencies

Individual agencies administer the final layer of security through their agency eVA security officer. General Services delegates specific responsibilities to the agency security officers. There are two levels of security delegation, basic and advanced.

Currently, most agency security officers retain the basic designation and are responsible for approving user access changes and sending them to the global security officer for implementation. They also coordinate user account management, which involves:

- determining whether user access is appropriate given current job responsibilities;
- ensuring user access for terminated employees is promptly deactivated and coordinating approval workflow changes once deactivated;
- conducting quarterly reviews of user accounts for reasonableness;
- ensuring users understand and adhere to security policies and authorized use of eVA; and
- implementing required policies, procedures, and processes within their agency to meet these responsibilities.

Similar to the global security officer, the agency security officer bears responsibility for facilitating and monitoring their agency's use of eVA and compliance with applicable federal and state statutes and policies.

General Services delegates advanced security functions to an agency after they fulfill specific requirements outlined in the eVA Security Manual (Security Manual). Advanced responsibilities include the ability to make user access changes and assign approval workflow roles to users.

As of May 2005, only 3 out of 171 state agencies have requested and been delegated advanced security functions. It is General Services' goal to delegate advanced security functions to agencies that have sufficient, qualified resources to fulfill these responsibilities.

RECOMMENDATIONS AND FINDINGS

Overall, General Services designed eVA security management well, but they have not fully implemented its design. Agencies continue to rely on General Services to administer security and provide them direction for their configuration rather than becoming self-sufficient. Further, General Services' actions, or lack thereof, has continued to foster the agencies' reliance on them. General Services needs to develop a strategy to transition qualified agencies to advanced security delegation.

To increase independence, General Services must improve their central monitoring efforts, provide monitoring tools to agencies, conduct periodic training and assessments of agency security officers, and update the Security Manual regularly. Without these improvements, it will be difficult for General Services to realize the goal of advanced security delegation. We address these issues in detail below.

Monitoring Activities

The Security Manual places significant monitoring responsibilities on General Services, ranging from user access to ensuring the solution complies with federal and state statutes and policies. However, General Services' current monitoring activities are limited and focus on a few key user access risks identified during initial user creation or subsequent user changes.

As the eVA environment has begun to stabilize, General Services has placed greater responsibility on each agency for their eVA configuration and would like to place greater responsibility for security. At the

same time, the tools that would allow agencies to monitor their security are weak and General Services has experienced significant turnover in their account executives, which affects the timing and quality of guidance and information they provide.

Further, CGI-AMS and their subcontractors offer their procurement solution to companies throughout the world. They designed this solution to appeal to the needs of all their customers, limiting the Commonwealth's ability to customize the solution. Thus, eVA offers capabilities that may conflict with Commonwealth policies and procedures. As an example, eVA allows purchase cardholders to share their card with other users in a manner that does not follow Commonwealth policies. This conflict between available functionality and policy requires General Services and agencies to monitor users diligently for compliance.

We found that General Services does not perform proactive regular reviews for inappropriate access or unauthorized activities and has not expanded their initial monitoring tools. In addition, they are not performing periodic assessments of agency's security practices and their compliance with the Security Manual. Instead, they are relying on the agency security officer to review user access quarterly for reasonableness. In addition, General Services is assuming agencies understand their eVA configuration sufficiently to accurately assess compliance with state and federal policies and procedures.

We worked with General Services staff to develop exception-based queries of eVA security set-up, which identified various instances of non-compliance that central monitoring could prevent. Prompt and accurate management of user access, roles, and privileges is essential in assuring the integrity of eVA transactions. Each instance of non-compliance we identified could negatively affect eVA.

For example, we found instances where agencies did not remove terminated employees, with some remaining active for up to one year past termination. In addition, we found users who had not used their accounts for over 30 days. Allowing terminated employees or inactive users to remain active presents a risk since users can buy via any internet connection. Although strong approval workflow mitigates these risks by requiring purchases to go through various approvals, the existence of terminated and inactive user accounts opens eVA to the risk of unauthorized transactions.

We also identified instances where agencies inappropriately assigned approval workflow and in some instances, had not assigned approval workflow at all. While employees had not used most of the accounts involved, the fact that accounts exist without proper or no approval workflow demonstrates the lack of monitoring or awareness by General Services and the agencies.

Finally, our queries found employees that set up other employees to share their purchase cards. Upon further review, we learned that CGI-AMS and General Services support staff informed agencies of this functionality, but not the implications of its use or that it was in violation of Commonwealth policies. While agencies bear a responsibility for compliance with all Commonwealth policies and procedures, General Services lack of monitoring tools to facilitate identifying instances of card sharing hampers the agencies' ability to ensure compliance.

Develop Monitoring Tools

General Services should use the queries designed during this audit and design additional exception-based queries to identify instances of inappropriate access or unauthorized activities. General Services should run and analyze these queries on a regular basis and work with the agencies to resolve exceptions promptly. Further, General Services should communicate the exceptions and their resolution to the agency security officers to help eliminate similar issues in the future.

When designing exception-based queries, General Services should consider involving members of the eVA community as well as central agencies who are responsible for policies and procedures that affect eVA, such as the Department of Accounts, who administers the purchase card program. These resources may provide insight into global, as well as agency specific, configuration risks.

As these monitoring tools are refined, General Services should consider making them available online to agency security officers and other appropriate central agencies. This will enable the agency security officers to more efficiently and effectively meet their monitoring responsibilities and the Department of Accounts to better manage the purchase card program. The distribution of such tools should coincide with appropriate training regarding their use.

Review Agency Security Practices for Compliance

As required by the Security Manual, General Services should periodically assess agency security practices and their compliance with the Security Manual. This will enhance global monitoring activities and the delegation of advanced security functions by allowing General Services to assess the agencies' understanding and identify areas requiring training.

We recognize that this is a resource intensive process. General Services may need to use resources outside of the Global Security office, such as the eVA account executives, to perform these reviews. The delegation of advanced security functions to more agencies may free up some of General Services' internal resources needed to perform these assessments, but will also increase the need for these assessments.

Security Awareness Training

General Services provided formal security awareness training to agencies in 2002, but they have not repeated it since. Limited security awareness discussions have occurred during the General Services' Public Procurement Forum; however, this conference targets the buyer and vendor communities. Consequently, there is no guarantee that an agency's security officer attends or will elect to participate in the sessions addressing security. General Services has instead relied on the Security Manual and one-on-one communication through account executives to address specific concerns. However, given their limited monitoring program, General Services depends heavily on agencies to identify their own needs.

While one-on-one communication may address specific areas of concern, it does not ensure that General Services delivers a consistent or timely message. In addition, General Services has experienced significant turnover within their account executive staff, potentially compromising the quality of the communication.

During our review, we interviewed a limited number of agencies. We observed a general lack of awareness or understanding of their overall eVA set-up and many requirements specifically addressed by the Security Manual. While this lack of awareness does not appear to have resulted in agencies processing fraudulent transactions, it does increase the risk that this will occur. In addition, it will prevent an agency from receiving delegated responsibility for eVA configuration and security administration and delay General Services overall goal of placing these advanced security functions at the agency level.

Conduct Regular Security Awareness Training for Agency Security Officers

General Services should provide formal eVA security training to agency security officers on a regular basis via on-line or in-house sessions. General Services should design these training classes to inform agency security officers about specific requirements in and changes to the Security Manual, address specific concerns identified by global security's enhanced monitoring process, and provide information on how to use monitoring tools.

In addition, General Services should develop a formal strategy for realizing their overall goal of delegating advanced security functionality to agencies. They should design their training program to facilitate the delegation strategy's execution.

eVA Manuals

General Services and CGI-AMS have issued multiple manuals discussing functionality, as well as security administration. All of these manuals are available in multiple locations on the eVA portal. Over time, General Services has developed operating procedures not contained in these manuals. During our review, we identified several areas where General Services could enhance or update their policies and procedures to reflect current practices.

For example, as agencies experienced turnover, unique concerns relating to user ID deactivation and its impact on approval workflow have arisen. The Security Manual requires agencies to deactivate user access within one working day after a user transfers, terminates, or changes responsibilities. Although this policy supports best practices, immediate deactivation of an account could prevent purchases in the workflow pipeline from processing, causing the order to be re-entered, have unexpected delays, or potentially resulting in duplicate orders.

Consequently, General Services has developed specific procedures to prevent terminated users from accessing eVA yet allowing time to resolve the approval workflow issues. The Security Manual does not incorporate these appropriate procedures. As a result, in most cases, user deactivations do not comply with existing policies and procedures.

As another example, eVA's design empowers users to manage their own shopping access. eVA's approval workflow ensures supervisory approval of user access changes and potentially requires agency security officer and global security officer approval based on the request. However, changes initiated outside of eVA, such as adding a new user, do not have the same approval requirements.

Specifically, the Security Manual and user access request form included in the manual do not address or require documentation of agency approvals. While the Security Manual requires agencies to implement procedures necessary to meet their security responsibilities, the agencies we interviewed have not established security policies above those provided in the Security Manual. Therefore, the audit trail supporting the approval of user access changes is lacking.

As mentioned above, General Services' long-term goal is to delegate advanced security functions. General Services has addressed this concept in the Security Manual, which describes the requirements to receive advanced delegation. However, as actual delegations have begun, General Services has identified reasons for delegating other critical administration functions and developed procedures outside the Security Manual to execute these delegations. To realize the goal of delegating advanced security functions, as well as advanced administration functions, agencies need to understand the additional types of delegation that are emerging and the knowledge, skills, and abilities they must demonstrate to receive these delegations.

We also reviewed, on a limited basis, the other eVA user manuals available on the portal. General Services issued these manuals beginning in March 2001 and may or may not have updated them. CGI-AMS was predominantly responsible for the manuals design and content and, in some cases, their instructions may conflict with Commonwealth policies and procedures.

For example, the manual entitled, “eVA Credit Card – Password – email Maintenance User Guide,” provides guidance for a user to share their purchase card with others. Small Purchase Charge Card policies and procedures outlined in the Commonwealth Accounting Policies and Procedures manual specifically prohibit the sharing of purchase cards, with one minor exception. The functionality described in this manual does not fall under this exception and as noted above, we identified instances where agencies are using this functionality.

Although agencies have a responsibility to ensure compliance with all Commonwealth policies and procedures, it is not surprising that they are taking advantage of non-compliant functionality as there is no warning or guidance within the manual concerning its use. General Services should provide agencies additional information concerning non-compliant functionality and the implications of its use.

Update and Enhance eVA Manuals

General Services should ensure that they reflect changes to operating procedures timely in the Security Manual. At a minimum, General Services should update the Security Manual to reflect policy changes they have already made in the following areas:

- Password requirements
- Deactivation of user accounts
- Delegation of eVA advanced security and administration functions

General Services should develop additional policies and incorporate them into the Security Manual in the following areas:

- User account change requests initiated outside of eVA
- Rescission of delegated authority

Further, the Security Manual recognizes the Virginia Information Technologies Agency (VITA) and its potential impact on future security management activities. However, the Security Manual was written prior to VITA’s formal creation and as such, does not fully reflect actual VITA operation decisions that have occurred. Global Security should work with VITA to better define their role in eVA’s security management and reflect the results of those discussions in the Security Manual.

Finally, General Services should review the various eVA manuals to identify functionality that conflicts with existing Commonwealth policies and procedures. Where this functionality exists, General Services should remove the instructions from the manual or add warnings that the Commonwealth does not authorize the functionality for use and agencies should contact their eVA security officer or account executive if they have questions.



Commonwealth of Virginia

Walter J. Kucharski, Auditor

**Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218**

June 14, 2005

The Honorable Mark R. Warner
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Lacey E. Putney
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have completed a review of eVA's user access and approval workflow management and submit our report entitled, "eVA Security Administration" for your review. We conducted our overall review in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

Objectives

The objectives of our review were to:

- review and document the processes used to administer and manage eVA security;
- determine whether General Services centrally manages eVA security in accordance with their policies and procedures; and
- determine whether agencies manage eVA security in accordance with policies and procedures.

Scope and Methodology

We conducted this review by interviewing General Services' and other agencies' personnel, reviewing policies and procedures, and evaluating agency compliance with Commonwealth policies and procedures. We determined the responsibilities of the central and agency security officers, assessed the types of monitoring and management activities performed, and evaluated the adequacy eVA's overall security administration.

In addition, we worked closely with General Services staff to gain an understanding of eVA's sensitive access privileges, approval workflow scenarios, and critical risk areas. We used this information, with the help of General Services staff, to develop detailed security queries that did not previously exist to detect inappropriate use and security violations.

Results

General Services has worked hard to implement a statewide procurement system that is accessible by anyone in the Commonwealth's buyer and vendor communities. The approach and methodology has earned them national recognition.

While the implementation of all the application's functionality is close to completion, General Services' work is not complete. Much of the early efforts with eVA focused on the transfer of knowledge from CGI-AMS and their partners to General Services. General Services has stated their ultimate goal is to delegate security administration functions to the agencies. General Services now needs to focus on completing the transfer of security administration knowledge to the agency security officers.

General Services has laid the foundation for this transfer by establishing strong policies and procedures and initiating lines of communication through their account executives. However, they need to build upon this foundation through full implementation of their policies and procedures and development of a security administration transition strategy. The security administration transition strategy should specifically identify the knowledge to transfer, the means of transferring the knowledge (i.e., training, newsletters, security officer user meetings), and the dates for transition.

As a part of this review, we also identified key areas within their eVA policy and procedure implementation that General Services could improve, including monitoring of user access and agency security administration, security awareness training programming, and updating or refining user guides and the Security Manual. By improving each of these areas, General Services will move closer to their overall goal of delegating advanced security functions to the agencies while ensuring the integrity of eVA.

We discussed this report with the Department of General Services on July 7, 2005. We have included their response at the end of this report.

AUDITOR OF PUBLIC ACCOUNTS

KKH/kva



COMMONWEALTH of VIRGINIA

Department of General Services

James T. Roberts
Director

July 7, 2005

202 North Ninth Street
Suite 209
Richmond, Virginia 23219-3402
Voice/TDD (804) 786-3311
FAX (804) 371-8305

Mr. Walter J. Kucharski
Auditor of Public Accounts
PO Box 1295
Richmond, Virginia 23218

Dear Walter:

The Department of General Services appreciates the time and effort the Auditor of Public Accounts staff spent reviewing eVA Security, and the opportunity to comment on the draft report. We are in substantive agreement with their findings, and hope to continue our collaboration as we address the report's recommendations.

eVA, as with all statewide applications, to be secure requires all aspects of the commonwealth to actively participate in securing eVA. As noted in the report, the eVA Security Manual places a high level of responsibility on the agency to follow good security practices. This responsibility is placed within the agency, because only the agency has visibility over staff changes and terminations. To support DGS in our efforts to improve the monitoring of eVA, it is our hope that APA will include eVA security in their agency audit plans and continue to work with the eVA team in developing meaningful monitoring reports.

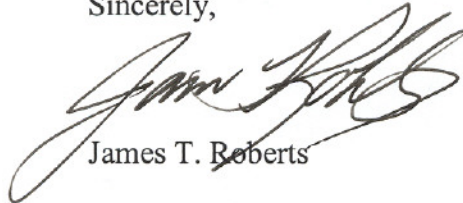
Based on the report's recommendations DGS has done the following:

- The Division of Purchases and Supply added review and approval of all eVA manuals by the DPS policy workgroup to its change control procedures.
- The Department of General Services has hired a Certified Information Security Professional to guide the department in the redrafting of the eVA security manual and the development of an eVA Security awareness program.
- The core eVA project team has conducted over 20 hours of in-service training for newly hired account executives
- By September 2005, the eVA team will post a set of monitoring reports for use by all agency security officers

- Upon release of this report, DGS will request VITA Security to include monitoring of compliance with the eVA security manual in their agency security audits.

DGS will continue to implement the intent of each of these recommendations within eVA's resource and financial constraints.

Sincerely,

A handwritten signature in black ink, appearing to read "James T. Roberts", written in a cursive style.

James T. Roberts