US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Audit of Integrated Financial and Acquisition Management System Access Controls

Audit	25-00529-219	February 17, 2026

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

vaoig.gov/hotline | 800.488.8244

OUR MISSION

To conduct independent oversight of the Department of Veterans Affairs that combats fraud, waste, and abuse and improves the effectiveness and efficiency of programs and operations that provide for the health and welfare of veterans, their families, caregivers, and survivors.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Visit our website to view more publications.
vaoig.gov

Executive Summary

The VA Office of Inspector General (OIG) initiated this audit to determine whether Integrated Financial and Acquisition Management System (iFAMS) user access controls, which are intended to limit account privileges, are sufficient to safeguard VA data and comply with applicable laws, regulations, and guidance. The audit scope focused on users who had access to acquisition-related data because of its sensitive nature. The team analyzed the accesses requested, the process followed to grant roles in iFAMS, quality reviews, and select user access requirements through May 2025.[1] Generally, the team found that access to sensitive acquisition information was not properly controlled for certain iFAMS users.

The OIG made three recommendations to refine iFAMS access controls, to periodically review and certify all roles and access, and to implement a permanent solution to allow supervisors and information owners to review user roles and access. In late October 2025, VA concurred with all three recommendations in the report. Specifically, VA reported new roles will be implemented for finance staff to limit access by fund code, and VA is replacing the legacy access system with an updated system that can include default access roles in the semiannual quality reviews. Additionally, VA plans to implement a future iFAMS enhancement that will include additional security features. Finally, once the updated system is successfully integrated, VA expects to include default access roles in the semiannual quality reviews and to develop an implementation strategy for deployment to all users based on VA’s priorities.

What the Audit Found

As part of the system’s financial-related functionality, iFAMS contains sensitive acquisition information like pricing and labor rates. This information must be protected as part of the principle of least privilege, which ensures only those users who need the information to complete assigned tasks have access to it. From a sample review of 20 iFAMS users, the OIG found that system access was not sufficiently limited as required for all users sampled, presenting a risk of unnecessary access to sensitive acquisition information.

This risk occurred, in part, because iFAMS access controls were too broad, making it difficult for supervisors and organizations to grant users access only to what they need. Additionally, quality reviews, which are intended to routinely ensure the appropriateness of user access, did not include all necessary information for reviewers to validate all access granted. In other words, the quality reviews do not capture all access that is granted to a user. Furthermore, Identity and Access Management, the electronic tool that allows supervisors and information owners to

[1] For more on this report’s scope and methodology, see appendix A.

routinely see user roles and accesses, does not show all accesses the users have been granted and therefore does not support comprehensive oversight.

Unnecessary access could compromise sensitive acquisition data within iFAMS. Also, with every additional user who can access sensitive information, the risk of misuse increases. If users have access to sensitive information, they, along with anyone else who gains access to their account, can use this access for personal gain. VA data could be subject to unnecessary risk in instances of compromised accounts or insider threats. This risk has the potential to compound as iFAMS continues to be deployed across VA.

Next Steps

The OIG found the action plans were responsive to the intent of the OIG recommendations, and VA plans to complete those actions by May 2026.[2] The OIG will continue to monitor VA's progress and will close the recommendations when VA has provided sufficient evidence that the corrective actions have been adequately implemented.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[2] See appendix C for the VA management comments in full.

Contents

Abbreviations

FMBT	Financial Management Business Transformation
IAM	Identity and Access Management
iFAMS	Integrated Financial and Acquisition Management System
OAL	Office of Acquisition and Logistics
OIG	Office of Inspector General
TAC	Technology Acquisition Center

Introduction

VA established the Financial Management Business Transformation (FMBT) program in 2016 to modernize its financial and acquisition systems. Through the FMBT program, VA is implementing the Integrated Financial and Acquisition Management System (iFAMS), a comprehensive system of record intended to replace multiple systems, with the goal of increasing transparency, accuracy, and timeliness, among other things. VA's FMBT Service is the office that oversees the deployment of iFAMS, which is occurring in phases, or "waves." The first wave to "go live" took place in November 2020.[3] Since 2023, the VA Office of Inspector General (OIG) has reported on concerns with iFAMS related to program risk management, the system not meeting user needs, and missed opportunities for communication, among others.[4] The OIG also found that access controls were a risk.

The OIG conducted this audit to determine whether iFAMS user access controls that are intended to limit account privileges are sufficient to safeguard VA data and comply with applicable laws, regulations, and guidance. The team focused specifically on procedures and controls related to VA's Technology Acquisition Center (TAC) data and the users who had access to it.[5] These users were VA employees and contractors who were granted access to TAC information in iFAMS and fell into two groups. Group 1 included users who worked for the TAC. Group 2 included users who did not directly work for the TAC. For example, a VA Office of Information and Technology employee who requests acquisition information from the TAC would fall into group 2.

The TAC, which is under the Office of Acquisitions and Logistics, provides acquisition and program management expertise and support for the life cycle management of enterprise-wide information and technology solutions. The team's audit scope included only users with access to acquisition-related data because of its sensitive nature.

As part of the system's financial-related functionality, iFAMS contains sensitive acquisition information such as pricing and labor rates. In the past, VA's acquisitions leaders have noted security and access challenges with iFAMS affecting acquisitions staff—specifically, that

[3] The term "go live" refers to the first day personnel can use iFAMS.

[4] VA OIG, *Integrated Financial and Acquisition Management System Interface Development Process Needs Improvement*, Report No. 24-00645-84, April 24, 2025; VA OIG, *End User Concerns with Integrated Financial and Acquisition Management System Training*, Report No. 23-01287-20, January 9, 2024; VA OIG, *Improvements Needed in Integrated Financial and Acquisition Management System Deployment to Help Ensure Program Objectives Can Be Met*, Report No. 21-01997-69, March 28, 2023.

[5] The team took a risk-based approach to identify the scope of the audit and included only users from offices, programs, or entities within VA who had access to VA's TAC data. The team did not consider other data. For more on this report's scope and methodology, see appendix A.

unauthorized VA users have access to sensitive acquisition information resulting in significant risks including unprotected data.[6]

According to VA policy, VA is required to properly protect this information as part of the principle of least privilege, ensuring it is only accessible to users who need it to accomplish assigned tasks according to organizational mission and business functions.[7] This principle supports the ability to limit or contain the effect of a potential cybersecurity or privacy event by developing and implementing appropriate safeguards.[8] Along the same lines, VA policy also states that system components performing different missions or business functions will be isolated or separated when necessary to limit the flow of unauthorized information and provide the opportunity to deploy greater levels of information protection.[9] Furthermore, VA guidance emphasizes "zero trust" architecture, the goal of which is to prevent unauthorized access to data coupled with access control enforcement that is as precise or granular as possible.[10]

System Deployment Schedule and Estimated Cost

Seven iFAMS waves have gone live across VA as of June 2025, representing only about 3 percent of the total anticipated iFAMS users. Broadly, the system offers two types of functionality: One is related to financial activities, including capabilities needed to maintain budgets, some procurement and purchasing actions, and reporting. The other is related to acquisition activities and includes the ability to solicit, award, and modify contracts. Attachments and references in transactions housed in the system's financial-related functionality include sensitive acquisition information, such as pricing and labor rates.

According to FMBT Service's latest published deployment timeline (from September 2024), all wave deployments, including the Veterans Health Administration which comprises the majority of VA's anticipated iFAMS users, will be completed sometime in 2031.[11] The FMBT program's life cycle cost estimate as of November 2024 was about $8.6 billion. This estimate includes costs

[6] Office of Acquisition and Logistics Project Management Office, *Department of VA FMBT – iFAMS Enterprise Acquisition Module Future State Recommendation*, November 7, 2024.

[7] Although this report is focused on acquisition data because of its sensitivity, all VA information is subject to the principle of least privilege.

[8] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

[9] VA Directive 6500.

[10] For the purposes of this report, the terms "data" and "information" are used interchangeably. According to the National Institute of Standards and Technology, in a system with zero trust architecture, an "enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources (such as data and compute [*sic*] resources and applications/services) to only those subjects and assets identified as needing access." National Institute of Standards and Technology, Special Publication 800-207, *Zero Trust Architecture*, August 2020.

[11] The FMBT Service estimated 125,000 employees will use the system once fully implemented, with 115,000 being Veterans Health Administration employees.

to deploy the system across VA and a sustainment period for the system through fiscal year 2050.[12]

VA's Acquisition Offices and Administrations

VA has a department-wide acquisition function, which is housed in the Office of Acquisition, Logistics, and Construction, which is further broken down into three offices. One of which is the Office of Procurement, Acquisition, and Logistics. Three VA-wide acquisition offices fall under the Office of Procurement, Acquisition, and Logistics. The first is the National Acquisition Center, which supports healthcare requirements. The second is the Strategic Acquisition Center, which focuses on noninformation technology enterprise solutions. The third is the TAC, which provides business and contracting solutions for various VA major information technology programs. This report focuses on access to TAC information because it presents risk due to the overall number of VA users with access—including those who did not directly work for the TAC—and the amount of acquisition-sensitive data available.

Acquisition Office's Input for iFAMS Development

The Office of Acquisition and Logistics (OAL) Project Management Office is responsible for coordination with the FMBT Service and to help ensure iFAMS meets the needs of VA's acquisition workforce. The OAL Project Management Office is responsible for two committees. The first is the OAL Project Management Office Steering Committee, chaired by the VA senior procurement executive and staffed by heads of contracting activity of seven administration/staff offices. The second is the OAL Project Management Office Workgroup, chaired by the project manager of this office. This workgroup is staffed with representatives nominated by the administration heads of contracting activities.

User Security Profiles

A user's security profile defines what access they have in a system. In iFAMS, a user's security profile must include data access privileges appropriate and necessary for the user to perform their duties but only those privileges that are appropriate (the principle of least privilege). These access privileges are granted through security organizations and user roles. A user's security profile can have multiple security organizations associated with it, each of which provides access to financial and acquisition data. Security organizations, such as the TAC, allow users and data to be placed in logical groups. For example, users can be grouped by the organization they work for. A user's assigned roles determine whether that user can view, submit, edit, or approve the

[12] FMBT Service, Life Cycle Cost Estimate Report, November 25, 2024. This represents the most current cost estimate available as of the publication date of this report. The life cycle cost as of November 2024 includes costs for development, implementation, and sustainment operations.

financial and acquisition data they have access to. Figure 1 shows how a user's access is established.

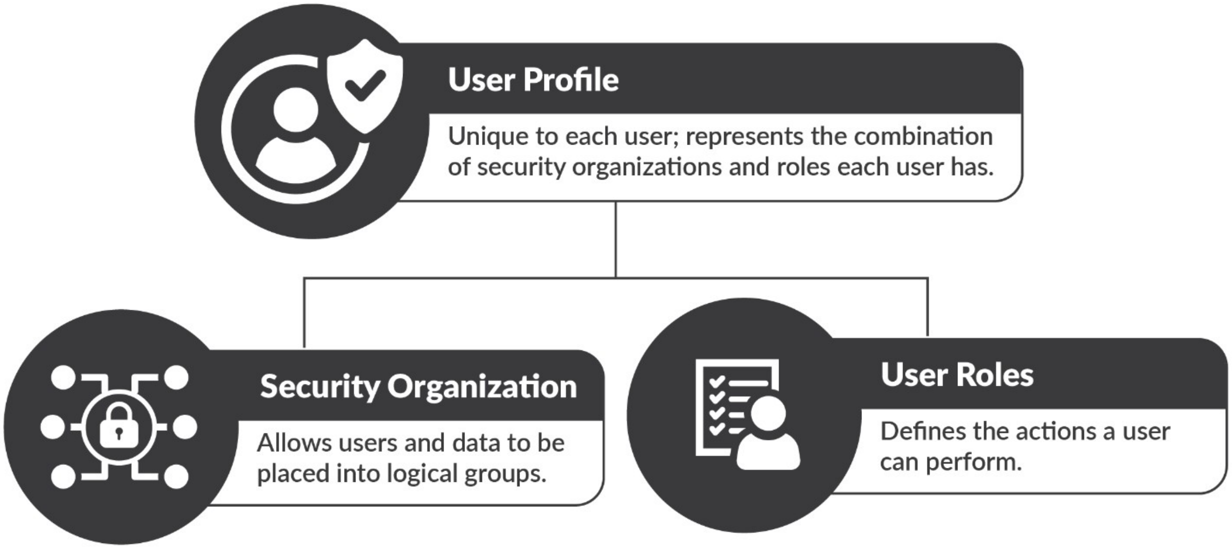

User Profile
Unique to each user; represents the combination of security organizations and roles each user has.
Security Organization
Allows users and data to be placed into logical groups.
User Roles
Defines the actions a user can perform.

Figure 1. *The elements that help establish user access.*

Source: VA OIG-created graphic using information from iFAMS History and Security Overview, August 5, 2024.

Access to data on a system—granted by the user's security organization and defined by the user's roles in that user's profile—is like access to a building. For example, a person can be granted access to an entire building, or just one floor of a building, or even just one room. The fewer places a person can access in a building, the more limited or precise that person's access is. Like accessing parts of a building, a user of a computer system such as iFAMS could access all or just some of that system's data.

Approval of User Security Profiles

VA's Financial Services Center iFAMS Accounting Systems Oversight Section team grants system access to establish a user's security profile in iFAMS. This team validates requests in VA's Identity and Access Management (IAM) system to approve and grant a user's security profile, which, as explained previously, includes the requested roles and security organizations. Users are generally granted access in one of two ways:

1. Access is requested during an iFAMS implementation wave, when a new employee is hired, or when position responsibilities have changed. Users can submit these requests for access, or supervisors or helpdesk staff can request access on the user's behalf and include documentation explaining why access is needed. These requests are typically routed to a supervisor, a person designated in an approval role by their organization, or both.

2. Separate from requested access, access can also be assigned. This is called default access and is predetermined during the wave's stakeholder integration process before go-live. A team of FMBT Service staff, leaders from the office about to go live, and system developers determines this default access based on what a user will need to complete their job duties.

Table 1 is an example of an iFAMS user who requested only one role but was ultimately granted three additional roles through the default access provisioning process. This user requested the "Standard View" role, which provides access to view all nonsensitive financial transactions. One of the additional roles granted ("Acquisitions View") allows a user access to detailed information supporting acquisition actions that may contain sensitive information.

Table 1. Example of Default Access Assigned to a User

Requested*	Role granted
Yes	Standard View
No	Acquisitions View
No	Standard View (Central Billed Account)
No	Reference Data

Source: VA OIG-created example based on iFAMS data.

* *"No" indicates default access.*

Users fall into two groups, which affects how access is approved. Group 1 users are VA employees and contractors who request access to information owned by the organization they work for. For instance, a TAC contracting officer requesting a role tied to the TAC security organization falls into group 1.[13] These user requests are reviewed by only one approver.

Group 2 users are VA employees and contractors who do not work for the organization from which they are requesting access to information. In contrast to the process for group 1, there are two levels of approval when these users request access to TAC information. Both the user's supervisor and the appointed acquisition supervisor for the TAC review these access requests. The user's supervisor reviews the request and determines whether the requested access is consistent with the user's job responsibilities. The acquisition supervisor then confirms the user should gain access to the requested information.

Although the FBMT Service refers to them as acquisition supervisors, these organizationally appointed individuals, such as those at the TAC, are also information owners. An information owner is any official with statutory or operational authority for information whose

[13] Throughout this report, the phrase "access to TAC" refers to users who have been granted access to the Head of Contracting Activity TAC security organization.

responsibilities include establishing controls to generate, collect, process, disseminate, or dispose of this information.[14]

Semiannual Reviews

Once users receive access to iFAMS, the FMBT Service enforces the principle of least privilege through semiannual quality reviews.[15] Depending on users' organizations, their semiannual reviews are either performed by their supervisor or by an appointed individual. For example, a VA business resource specialist involved with this process reported the TAC has appointed individuals who can perform this function. The Accounting Systems Oversight Section team tasks either supervisors or organizationally appointed individuals with reviewing and certifying the access of all users during the quality review, using a report containing access information for each user from the IAM system. The reviewers use this report to see what access the users have and to either certify, remove, or request changes to this access.

[14] National Institute of Standards and Technology, Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

[15] iFAMS System Security Plan, June 14, 2024. VA policy requires periodic reviews to certify users' continued need for access according to the iFAMS system security plan, which further defines the frequency of these reviews as "semiannual," or twice yearly.

Results and Recommendations

Finding: Gaps in Access Controls Left Sensitive Acquisition Information Vulnerable

The OIG found the FMBT Service's controls are not sufficient to ensure the principle of least privilege is consistently enforced, as required by VA policy.[16] Consequently, users have unnecessary access to view sensitive acquisition information.[17] To assess these controls, in January through May 2025, the audit team reviewed account privileges and related documentation explaining why access was needed for 20 users with access to TAC data, as of at least January 2025 (10 who worked for the TAC and 10 who did not).[18] The team determined user access was not sufficiently limited as required for all 20 users in the sample, presenting a risk of unnecessary access to sensitive acquisition information.

The team also assessed VA-wide user data and found 91 percent of the 2,818 users with access to the TAC data were VA employees or contractors who did not directly work for the TAC as of February 2025. Of those users not working for the TAC, 78 percent had roles that granted exceptionally broad access to sensitive acquisition information, including pricing and labor rates. Thus, the team determined there is widespread risk of users who do not work for the TAC having unnecessary access to sensitive acquisition information.

This risk of unnecessary access to sensitive acquisition information exists in part because the security organizations for acquisitions data, such as the TAC, are too broad to comply with least privilege requirements. Additionally, semiannual reviews to confirm whether users need the access granted to them were not comprehensive because they did not cover all user roles. Furthermore, IAM, the electronic tool that is available for supervisors and information owners to see user roles and accesses, does not support comprehensive oversight.

These findings highlight the widespread risk that sensitive acquisition information is vulnerable. Until access controls are enhanced and all roles and accesses are reviewed as required, VA will continue to be at risk of VA employees and contractors unnecessarily viewing or disclosing potentially sensitive acquisition information. This risk increases as iFAMS continues to be deployed across VA.

[16] VA Directive 6500.

[17] Specifically, the audit team identified risks with users' ability to view data, not their ability to edit or modify data.

[18] These users were VA employees or contractors.

What the OIG Did

The audit team analyzed the accesses requested, the process followed to grant roles in iFAMS, the quality reviews, and select user access requirements through May 2025. As part of the process to determine, in detail, how specific users received access to TAC data, the team examined documentation of the account privileges for a stratified random sample of 20 users with access to TAC data, as well as the two most recently completed quality reviews, as of at least January 2025.[19] The team reviewed 10 users who worked for the TAC and 10 VA users who did not work for the TAC. Then, for select users, the team reviewed documentation supporting what data they need to perform their duties. The team also employed a more general, data-driven analysis to identify, for all 2,818 users with access to the TAC as of February 2025, which organization they belong to and the nature of their role. The team also reviewed the current roles and authorities of supervisors and information owners.

The team interviewed FMBT Service staff, Financial Services Center staff, and other VA stakeholders and reviewed applicable criteria and procedures. The team also analyzed FMBT program documents and observed demonstrations of the provisioning process with the Accounting Systems Oversight Section team. Appendix A provides more information regarding the audit's scope and methodology.

Users' Broad Access in iFAMS

The OIG team determined user access was not sufficiently limited as required for all 20 users in the sample. As previously explained, the users sampled were VA employees and contractors who fell into two groups. Group 1 included users who worked for the TAC and group 2 included users who did not.

Users Who Worked for the TAC

The team found that all 10 users sampled who worked for the TAC had access to information beyond what was needed to complete their job duties. To make this determination, the team compared access to contract information in the legacy system to access in iFAMS. Across the TAC, there are over 8,000 active awards (contracts, orders, and modifications) in the legacy system. For all 10 users sampled who worked for the TAC, the team determined the awards assigned as part of each user's workload represented only a small portion of the total awards. For example, one user needed access to only 102 of the over 8,000 awards to complete their job duties. But, in iFAMS, all 10 of these users who worked for the TAC had access to all processed awards and orders associated with the TAC, not just those associated with their assigned workload.

[19] For more on this report's statistical sampling methodology, see appendix B.

Users at the TAC have a legitimate need to know some contract information to complete their job duties. However, access to all contract information in iFAMS does not comply with VA requirements to ensure it is only accessible to users who need it to accomplish assigned tasks (the principle of least privilege).

Users Who Did Not Work for the TAC

Because it was more difficult to determine what specific access was needed for users who did not work for the TAC, the audit team requested TAC information owners verify whether the 10 sampled users needed the access granted to them in iFAMS to complete their job duties. These users in the sample who did not work for the TAC had roles and access that had not previously been reviewed and approved by TAC information owners; they were granted access through another process, such as default access. Default access grants additional roles and access based on a user's organization and position, as agreed upon during the stakeholder integration process before go-live.

In response to the team's request, information owners said all users who did not work for the TAC would have been denied access if the TAC had reviewed these requests. The users would have been denied access for two main reasons:

- The roles requested gave users exceptionally broad access to TAC data.
- There was insufficient documentation explaining that this broad access was necessary for the users to complete their job duties.

The team was also told that these reasons were applicable, in general, to all users who do not work for the TAC—not just those included in the audit team's sample. Therefore, starting in November 2023, the TAC developed a practice to deny all user access requests from those who do not work for the TAC to help mitigate the associated risk.[20] However, without additional granularity of access, VA may be delaying and denying access requests from users who have a valid requirement for some of this information for their jobs.

As noted above, the OIG team confirmed all 10 users lacked appropriate documentation for the access granted. In some cases, the documentation was completely absent. In other cases, the documentation simply stated, "no comment provided." The team also confirmed seven of the 10 users had the Acquisitions View role, giving them broad access. As stated earlier, this view allows a user to access detailed information supporting acquisition actions. When granted in

[20] According to a TAC information owner, in April 2025, the FMBT Service provided the TAC with a list of 41 users who did not work for the TAC for TAC information owner approval for their initial provisioning as part of the Veterans Health Administration wave that was to go live in June 2025. The initial list of users was not approved by TAC leaders. However, after some coordination, TAC leaders concurred with providing temporary access to 11 users.

combination with TAC access, this role provides visibility of processed TAC awards and orders that may contain sensitive acquisition information.

The team determined that of the 2,818 active user profiles with access to the TAC, 2,562 were users who did not work for the TAC (91 percent) as of February 2025. In total, 1,992 of these users (78 percent) had the Acquisitions View role, which presents a widespread risk of users who do not work for the TAC having unnecessary access to sensitive acquisition information.

The information owners also told the audit team they cannot see all roles granted to users in iFAMS. This limited visibility increases the risk that users have unnecessary access because information owners do not know who a particular user is, cannot identify a particular contract that would authorize a user's access to contractual data, and cannot determine whether appropriate nondisclosure agreement documentation was signed under the contract that would allow access to obligation data.

iFAMS Security Organizations

A key factor contributing to users having more access than necessary is that the current security organization design is too broad and does not allow access to be limited only to what users need to perform their duties. That is, all TAC acquisition data are in one security organization—therefore, it is "all" or "none" access.

Security organizations allow users and data to be placed in logical groups to control access. When the security organization structure was being developed, TAC stakeholders expressed concerns to the FMBT Service about an initial proposal to define the security organization at the Office of Procurement, Acquisition and Logistics level. TAC stakeholders thought this would allow users of each of the acquisition centers (the National Acquisition Center, the Strategic Acquisition Center, and the TAC) to view each center's data. Responding to these risks, the FMBT Service proposed defining the security organization at the acquisition center level, which was the approach that was ultimately approved and implemented in April 2022. However, defining the security organization at the acquisition center level, the TAC in this case, was still too broad and did not fully mitigate the risk of users who do not work for the TAC potentially having unnecessary access.

Stakeholders coordinate with the FMBT Service on the details of how access controls, such as security organizations, are implemented for their data as part of the deployment of iFAMS at a new VA administration or office. One option to limit user access is to reduce the scope of security organizations during this coordination period. This could be done by implementing security organizations that further limit access.

Furthermore, iFAMS can support granular access controls. In March 2025, the FMBT Service began coordination with OAL Project Management Office acquisition stakeholders on an alternative design. The FMBT Service proposed adding more granularity to finance users' access to acquisition security organizations—that is, the ability to grant access to less information at a time. The OIG's first recommendation is for the FMBT Service to implement a plan with the OAL Project Management Office to ensure system access is more granular and the intent of the principle of least privilege is met.

Semiannual Quality Reviews of User Roles and Accesses

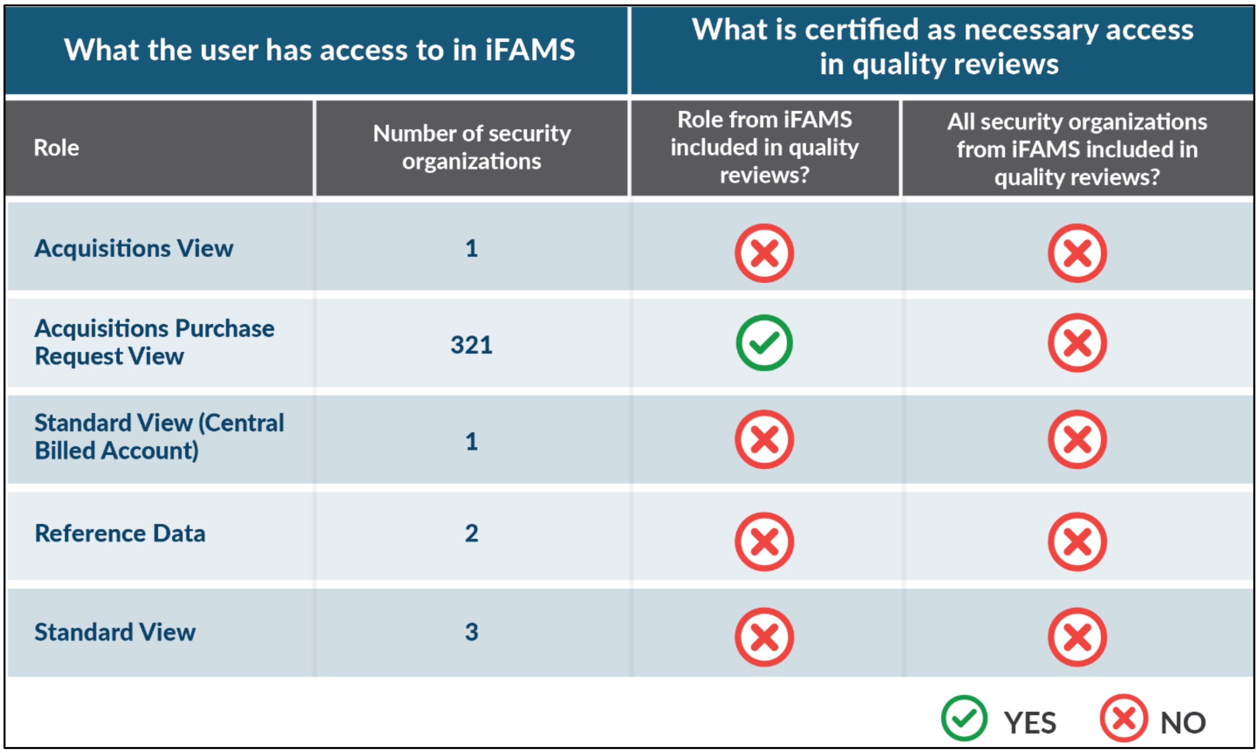
The iFAMS system security plan requires supervisors to conduct semiannual quality reviews to confirm whether users still need the access granted to them; during these reviews, any unnecessary access should be removed.[21] According to the Accounting Systems Oversight Section, quality reviews are the only routine control in place to ensure least privilege once initial provisioning has occurred.

In its evaluation of fiscal year 2024 quality reviews, the OIG team found that most user roles and accesses captured by the system were reviewed. But the system does not capture every role or access granted to each user. In other words, while the FMBT Service assessed user access through the quality reviews as required, these assessments did not include a review of *all* roles and accesses granted to a user. The 20 users the audit team sampled had a total of 129 roles assigned, as of February 2025. The team determined 79 of these 129 roles (61 percent) were not captured by the system and, therefore, were not checked during the quality reviews. For 29 of the 129 roles (22 percent), the accesses granted to users exceeded what was certified in the quality reviews.

For example, figure 2 shows the actual access granted to one of the users in the sample compared to what was certified during quality reviews. Only one of the user's five assigned roles, "Acquisition Purchase Request View," was checked during quality reviews. However, that role was only certified as required in the quality review for a single security organization, not the 321 security organizations associated with this user's role in iFAMS.[22]

[21] iFAMS System Security Plan. According to the iFAMS System Security Plan, "The review identifies when accounts are no longer required, users that are terminated or transferred, and when [a] user's information system usage or need-to-know changes."

[22] As of September 2024, there were 371 total security organizations in iFAMS.



What the user has access to in iFAMS		What is certified as necessary access in quality reviews	
Role	Number of security organizations	Role from iFAMS included in quality reviews?	All security organizations from iFAMS included in quality reviews?
Acquisitions View	1	✗	✗
Acquisitions Purchase Request View	321	✓	✗
Standard View (Central Billed Account)	1	✗	✗
Reference Data	2	✗	✗
Standard View	3	✗	✗

✓ YES ✗ NO

Figure 2. *Comparison of one user's access in iFAMS to what was evaluated during quality reviews.*

Source: VA OIG assessment of user access in iFAMS and quality reviews.

Without a comprehensive review of user access, VA cannot effectively guarantee the principle of least privilege is continually followed. The OIG's second recommendation is for the FMBT Service to ensure all roles and accesses are reviewed and certified periodically as required.

The Electronic Tool Used for Oversight

Supervisors did not review every role and security organization associated with each user, in part, because the electronic tool available to them did not capture all relevant information. According to FMBT provisioning guidance, access to iFAMS is granted through the IAM tool. Supervisors and information owners need to routinely review user roles and accesses in IAM as part of their ongoing oversight role. This is also the system where supervisors and information owners review and approve access requests. However, despite IAM's role in granting access, this tool does not show all user accesses granted in iFAMS. Figure 3 illustrates the differences between what a supervisor can see in IAM and what access a user actually has in iFAMS.

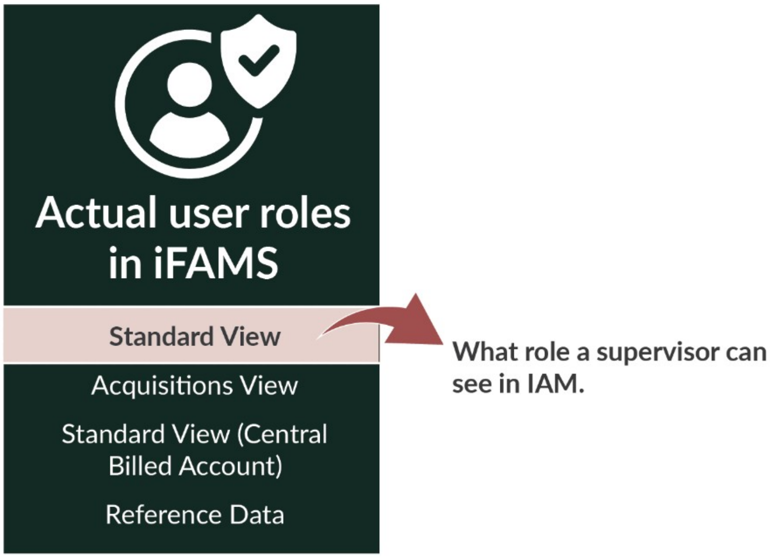

Actual user roles in iFAMS
Standard View
Acquisitions View
Standard View (Central Billed Account)
Reference Data
What role a supervisor can see in IAM.

Figure 3. *Comparison of what roles a user has in iFAMS and what their supervisor can see in IAM.*

Source: VA OIG-created example.

IAM does not provide supervisors and information owners with a complete picture of a user's actual iFAMS roles and accesses on a routine, ongoing basis. As noted in figure 3, a supervisor or information owner could only see the "Standard View" role when reviewing a user's access, since IAM does not reflect all roles granted in iFAMS. Similarly, TAC information owners could not see all the iFAMS roles for the users in the OIG's sample. For example, only the 256 users who work for the TAC of the 2,818 total users are visible to TAC information owners in IAM. TAC information owners do not know how many users who do not work for the TAC have access to their data. According to an Accounting Systems Oversight Section employee, this access was largely coordinated with the users' organizations as part of their stakeholder integration process. Sensitive acquisition data remain vulnerable to improper access if users' roles and accesses are not reviewed for least privilege by information owners.

FMBT Service leaders told the audit team that, as of April 2025, VA is considering procuring a new identity and access management system to replace IAM. FMBT Service leaders anticipate this solution may address the inability for supervisors and information owners to review all access granted in iFAMS. Nevertheless, to improve oversight of access, the OIG's third recommendation is for the FMBT Service to implement a permanent solution to provide supervisors and information owners with visibility of all roles and access granted to users.

Risks of Unnecessary Access to Sensitive Information

The controls reviewed in this audit do not sufficiently limit data access to only those with a legitimate need, which increases the risk of data being compromised. With every user who has access to sensitive information, the risk of misuse increases. If users have access to sensitive information, they, along with anyone else who gains access to their account, can use this access for personal gain. In other words, if their account was compromised or they were an insider threat, VA data would be subject to unnecessary risk. With each additional role or access granted, this risk increases. According to a functional iFAMS expert, the system has an audit trail that provides a history of what changes were made to a given document or transaction and who made them. But the system does not capture who may have improperly viewed sensitive information. This makes preventing unnecessary VA access through enforcing the principle of least privilege even more critical.

Furthermore, because TAC information owners cannot see all access to their information in an on-demand fashion, and without an enduring role in reviewing users for access, information owners cannot help VA certify that users continue to need the access they are granted. As previously mentioned, iFAMS has gone live for only about 3 percent of the total anticipated iFAMS users as of June 2025. Without improvements to controls, VA is not fully complying with internal policy and federal mandates. Additionally, VA does not have reasonable assurance that these security risks will not grow in future deployment waves.

Conclusion

VA does not have adequate controls in place that provide the department with reasonable assurance that users have access to only what they need to perform their duties, as evidenced by the unnecessary access to data identified in the OIG's sample review. This unnecessary access—or even the risk of it—could compromise sensitive acquisition data in iFAMS. Further, this problem could compound as more VA staff are added to iFAMS with each new wave. In the future, the FMBT Service should work with VA acquisition leaders toward a solution that grants access at a more granular level to limit risk. Additionally, the FMBT Service should ensure all user roles and accesses are reviewed and that all necessary stakeholders are part of this review. By improving the provisioning process and oversight tools, the FMBT Service can ensure compliance with VA regulations and consistently enforce the principle of least privilege.

Recommendations 1–3

The OIG recommends the deputy assistant secretary for the FMBT Service conduct the following actions before the next scheduled iFAMS implementation wave:[23]

1. Implement a plan with the Office of Acquisition and Logistics Project Management Office to ensure system access is more granular and the intent of the principle of least privilege is met.

[23] The FMBT Service administers the program (FMBT) to implement iFAMS, which is led by the deputy assistant secretary. The recommendations addressed to the deputy assistant secretary are directed to anyone in an acting status or performing the delegable duties of the position.

2. Ensure all roles and accesses, including those provided by default access, are reviewed and certified periodically as required.
3. Implement a permanent solution to provide supervisors and information owners with visibility of all roles and accesses, including those provided by default access, granted to users.

VA Management Comments

In October 2025, the principal deputy assistant secretary for management and deputy chief financial officer concurred with all three recommendations. For recommendation 1, the principal deputy assistant secretary reported that an enhancement to iFAMS will be implemented to add two new roles specifically for finance staff to limit access by fund code.

For recommendation 2, he stated that VA is replacing the legacy access system with an updated system that can include default access roles in the semiannual quality reviews. Additionally, a future iFAMS enhancement will include a secondary security organization. Once implemented, the two new roles and accesses limited by fund code will be included in the semiannual quality reviews for all finance users, which will be reviewed and approved by finance supervisors.

To address recommendation 3, the principal deputy assistant secretary reported that once the updated system is successfully integrated, Financial Services Center expects to include default access roles in the semiannual quality reviews and will develop an implementation strategy for deployment to all users based on VA's priorities.

The principal deputy assistant secretary stated the corrective actions are targeted to be completed by May 2026. The full text of the response is included in appendix C.

OIG Response

The corrective action plans are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close recommendations when VA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified.

Appendix A: Scope and Methodology

Scope

The audit team conducted its work from December 2024 through July 2025. The audit scope includes a stratified random sample of Integrated Financial and Acquisition Management System (iFAMS) users from a population of users from other offices, programs, or entities in VA who had access to the Technology Acquisition Center (TAC) data from June 12, 2023, through July 18, 2024.[24] The team verified these users still had access to iFAMS in January 2025 and considered documentation through May 2025. The team also considered a risk-based selection of access controls and associated documentation regarding managing user provisioning. The audit scope included only users with access to acquisition-related data because of its sensitive nature. On February 21, 2025, the team also obtained TAC access reports that were iFAMS generated, in real-time. The team also assessed the process by which the Financial Management Business Transformation (FMBT) Service facilitated the review and certification of user needs for access.

Methodology

The team reviewed applicable laws, regulations, policies, procedures, and best practices related to information privacy and security, internal control, information system risk management, and identity, credential, and access management. The team also obtained and reviewed relevant iFAMS documentation including

- system assessment and authorization documents, such as the iFAMS authorization to operate decision document, system security plan, and privacy impact assessment;
- user provisioning workflows;
- concept documents outlining the system’s security history and overview;
- inventories of system security roles and security organizations;
- records of fiscal year 2024 quality reviews documenting VA’s approach to monitoring users’ needs for system access;
- security organization access reports that identified 2,818 users with access to TAC data, as of February 2025;
- associated job aids and guidance to understand the user provisioning and quality review processes; and
- support for TAC user access requirements as of May 2025.

[24] Throughout this report, the phrase “access to TAC” refers to users who have been granted access to the Head of Contracting Activity TAC security organization.

The team interviewed several iFAMS stakeholders, including FMBT Service officials, VA acquisition community employees, and contractors. To identify any gaps or potential internal control weaknesses, the team selected a random sample of 20 iFAMS users (10 users who worked for the TAC and 10 users who did not) with access to TAC data to evaluate the user provisioning process and subsequent monitoring for access. The team assessed access requirements for the 10 users who worked for the TAC to determine what data would be necessary to perform their jobs and coordinated with the information owners to assess the risks of unnecessary access for the 10 users who did not work for the TAC.

To analyze user access to the TAC security organization, the team also selected access reports on user information and security roles as of February 2025. The team analyzed the reports and classified users as either group 1 (those who worked for the TAC) or group 2 (those who did not work for the TAC) based on each security organization. The team calculated the number of unique users per security role and the number of unique users across all security roles and took precautions to avoid double-counting. The team concluded that the data contained 256 unique users in group 1 and 2,562 unique users in group 2, totaling 2,818 unique users with access to the TAC security organization.

Internal Controls

When internal control is significant within the context of the audit objectives, Generally Accepted Government Auditing Standards (Yellow Book) 9.29 requires auditors to report the following:

1. The scope of their work on internal control.
2. Any deficiencies in internal control that are significant based on the audit work performed.

The team assessed the five internal control components and their underlying principles: control environment, risk assessment, control activities, information and communication, and monitoring.[25] While every principle of internal control is important, the team identified two components and three principles as significant to the audit objective.[26] The team identified internal control weaknesses during this audit and proposed recommendations to strengthen those listed in table A.1.

[25] Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

[26] Since the audit was limited to the internal control components and underlying principles identified, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Table A.1. VA OIG Analysis of Internal Control Components and Principles Identified as Significant

Component	Principle	Deficiency identified by this report
Control activities	10. Management should design control activities to achieve objectives and respond to risks.	The FMBT Service could improve its quality review process by ensuring all roles and accesses are reviewed and certified periodically as required by supervisors and information owners.
Control activities	11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.	The FMBT Service could coordinate with acquisition stakeholders to ensure system access is more granular and the intent of the principle of least privilege is met.
Monitoring	16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	The FMBT Service could implement a permanent solution to provide supervisors and information owners with visibility of all roles and accesses granted to users.

Source: VA OIG analysis of internal control components and principles. The principles listed are consistent with the Government Accountability Office's Standards for Internal Control in the Federal Government.

Data Reliability

The team requested and received documentation for each stage of the employee provisioning and review process, both from VA's Identity and Access Management (IAM) system and iFAMS. Additionally, the team obtained walkthroughs of the provisioning process from the Accounting Systems Oversight Section team and documentation for how specific roles and accesses are added to user profiles. The audit team also observed the Accounting Systems Oversight Section team as they pulled requested reports and information and validated that the information received matched what was requested. The data used were determined to be reliable for the purposes of this audit.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on audit objectives. The OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Appendix B: Statistical Sampling Methodology

Approach

To accomplish the objective, the team reviewed a random sample of 20 iFAMS users (and their associated roles and accesses) from a population of users who were assigned a role associated with the TAC security organization from June 12, 2023, through July 18, 2024. The team verified these users still had access to iFAMS in January 2025 and reviewed associated evidence through May 2025.

Population

The review population included 2,306 iFAMS users who were assigned a role associated with the TAC security organization from June 12, 2023, through July 18, 2024.

Sampling Design

With the OIG statisticians, the team selected a stratified random sample of 20 iFAMS users with access to TAC data. Designation of primary security organization (those who worked for the TAC versus those who did not) is the stratification variable. Table B.1 shows the size of the review population and the sample corresponding to each stratum.

Table B.1. Sampling Strata

Stratum	Designation	Population size	Sample size
1	Worked for the TAC	223	10
2	Did not work for the TAC	2,083	10
Total		**2,306**	**20**

Source: VA OIG analysis of TAC iFAMS users, extracted from iFAMS in July 2024.

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: October 29, 2025

From: Principal Deputy Assistant Secretary for Management and Deputy Chief Financial Officer (004)

Subj: Office of Inspector General (OIG) Draft Report, Integrated Financial and Acquisition Management System Access Controls and Reviews Should be Enhanced (VIEWS 13830097)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to review the report titled Integrated Financial and Acquisition Management System Access Controls and Reviews Should be Enhanced. The Financial Management Business Transformation Service concurs with all recommendations and submits the attached action plan.

The OIG removed point of contact information prior to publication.

(Original signed by)

Edward J. Murray

Attachment

Attachment

Department of Veterans Affairs (VA)

Financial Management Business Transformation Service (FMBTS)

Management Comments on and Action Plan for

Office of the Inspector General Draft Report

"Integrated Financial and Acquisitions Management System Access Controls

and Reviews Should be Enhanced"

Project Number 2025-000529-AE-0024

Recommendation 1: Implement a plan with the Office of Acquisition and Logistics Project Management Office to ensure system access is more granular and the intent of the principle of least privilege is met.

Comments: Concur. A future Integrated Financial and Acquisitions Management System (iFAMS) enhancement will be implemented to add two new roles designed specifically for finance personnel with access limited by fund code. The enhancement will be deployed in May 2026, ahead of the Momentum 8.3 upgrade, and will meet the intent of the principle of least privilege.

Status: In-Progress

Target Completion Date: May 2026

Recommendation 2: Ensure all roles and accesses, including those provided by default access, are reviewed and certified periodically as required.

Comments: Concur. As noted in the audit report, the majority of user roles and accesses are reviewed through the Semi-Annual Quality Access Review (QAR) process; however, default access is not included in that review. Financial Services Center (FSC) developed an interim solution, but the current Department of Veterans Affairs (VA) access management system does not have the capability to display the detailed information comprising "default access."

VA is in the process of replacing the legacy access system with an updated system that will have the capacity to include default access roles in the Semi-Annual QAR. For more details, refer to the following response for Recommendation 3.

In addition, a future iFAMS enhancement, planned for May 2026, will include a secondary security organization. Once implemented, the two new roles and accesses limited by fund code will be included in the Semi-Annual QAR for all finance users, which will be reviewed and approved by finance supervisors.

Status: In-Progress

Target Completion Date: May 2026

Recommendation 3: Implement a permanent solution to provide supervisors and information owners with visibility of all roles and accesses, including those provided by default access, granted to users.

Comments: Concur. As noted in the audit report, the majority of user roles and accesses are reviewed through the Semi-Annual QAR process. However, the current VA access management system does not have the capability of displaying all roles and accesses.

VA is in the process of replacing the legacy access system with an updated system. FSC will ensure the requirement to display the details underlying default access is integrated into the new system during the pilot test scheduled for May 2026. Once successfully integrated, FSC expects to include default access roles in the Semi-Annual QAR and will develop an implementation strategy for deployment to all users based on VA’s priorities. FSC will provide updates once this strategy is developed.

Status: In-Progress

Target Completion Date: May 2026

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Audit Team	Jessica Blake, Director Shawn Gillis Reynaldo Gonzales Amanda Taylor
Other Contributors	Allison Bennett Charlma Quarles R. Rachelle Wang-Cendejas

Report Distribution

VA Distribution

Office of the Secretary
Office of Accountability and Whistleblower Protection
Office of Acquisition, Logistics, and Construction
Office of Congressional and Legislative Affairs
Office of General Counsel
Office of Management
Office of Public and Intergovernmental Affairs

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.vaoig.gov.