AUTHORITY

A.R.S. § 13-2316; 35-131; 41-722

II. INTRODUCTION

Application Security is the joint responsibility of each agency and the Department of Administration. It is the most important area of all automated or manual financial systems. Proper segregation of duties and security measures must be present. Security is the key to a complex system which integrates many hardware platforms and applications. Applications include HRMS, AFIS, BITS, etc. Security can be separated into the following areas:

- Mainframe Security
- Database Security
- Network Security
- Application Security

This section of the Accounting Manual will address accounting issues as they relate to Application Security only. The policies and procedures herein are established as a supplement to those addressing internal controls and must be followed accordingly. Refer to the HRMS Users' Manual for specific HRMS policies and procedures.

III. DEFINITIONS

A. ADOA - Arizona Department of Administration.

B. AFIS Security Administrator - designated by the director or agency head of each agency, this individual is responsible for overseeing the agency's AFIS security and for making all AFIS access requests to the appropriate section of the ADOA.

C. Arizona Financial Information System (AFIS) - the State of Arizona automated accounting and financial reporting system.

D. GAO Security - the group responsible for maintaining the statewide assets and financial systems application security tables (profiles).

E. General Accounting Office (GAO) - within the Arizona Department of Administration, Financial Services Division. The GAO is primarily responsible for establishing statewide accounting policies and overseeing the accounting functions of all State agencies.

F. Human Resource Management System (HRMS) - the State of Arizona automated payroll and personnel management system.

G. HRMS Security Administrator - designated by the director or agency head of each agency, this individual is responsible for overseeing the agency's HRMS security and for making all HRMS access requests to the appropriate section of the ADOA.

H. ISD Information Services Security (ISD/ISS) - the group of individuals responsible for the initial setup of users on the mainframe security package (RACF) and providing users with access to the AFIS databases.

I. Information Services Division (ISD) - within the Arizona Department of Administration, formerly the Information Resource Management Group (IRMG).

J. Resource Access Control Facility (RACF) - proprietary IBM Computer Operating System security system.

K. User ID - an individual's personal data access control identifier.

IV. POLICIES AND PROCEDURES

A. Internal Controls

1. Agency management is responsible for maintaining a system of internal controls that minimizes the risk of errors and irregularities.

2. Internal controls must be a high priority of every agency.

3. All financial and accounting responsibilities should be segregated so that no one individual has complete control over an entire transaction.

   For example, no AFIS user should have the ability to add vendors to the vendor file, enter claims, release claims and have physical access to the warrants. At a minimum, one of these functions should be segregated to ensure that more than one person has reviewed each transaction.

4. All Personnel and Payroll responsibilities should be segregated so that no one individual has complete control over both the hiring and paying processes.

   For example, no HRMS user should have the ability to add an employee to the system or modify an employee's information, process supplementals or time and attendance, have access to or pick up the warrants, and perform the review of the payroll reports.

5. Segregation of duties is intended primarily to reduce the situations under which an individual might have the ability to perpetrate and conceal errors and irregularities in the normal course of duties. No one should be in a position to be tempted by or accused of inappropriate activity.

6. When segregation of duties is not possible at an agency (i.e., a very small agency), the agency may establish alternate procedures which control the risk of unauthorized transactions. These procedures must be written and well-documented.

7. Review procedures should be in place to prevent and detect any errors or irregularities. The warrant register and daily control reports should be reviewed on a daily basis by someone independent of the input and release functions. Once the reports have been reviewed, the reviewer should initial and date the reports. This will provide evidence to any future reviewer or auditor that the review was performed. Refer to the AFIS Reference Guide (Chapter 6) for additional information regarding review procedures.

8. For additional information or assistance in establishing internal controls, refer to the General Internal Control section of this Manual or contact your GAO Liaison.

B. Security Administrator

1. The agency head must designate an individual to act as the agency's AFIS Security Administrator and an individual to act as the agency's HRMS Security Administrator. The designation must be documented on a GAO-3 and accompanied by a memo stating why the individual is capable of handling the duties and responsibilities associated with being the AFIS and/or HRMS Security Administrator. The notification shall be sent to the GAO and kept on file by the GAO Security group. (At the discretion of the agency head, one individual may be designated to act as both AFIS and HRMS Security Administrator.)

2. The Security Administrator must be aware of factors affecting internal control such as AFIS and/or HRMS access of each employee, signature authorization of each employee, which employees in the agency have a Warrant Authorization Card (WAC) or have physical access to processed warrants, and which employees perform reviews and reconciliations of the AFIS and payroll reports.

3. The Security Administrator should possess at least a basic understanding of the AFIS and/or HRMS but his/her access to the system should be limited to inquiry only. The individual designated as the Security Administrator should complete the applicable Security Administrator Training, provided by the GAO, prior to performing duties.

4. The Security Administrator's responsibilities include, but are not limited to, the following:

   - Creating and maintaining a secure operating environment within his/her agency in order to prevent errors and irregularities;
   - Approving and submitting requests to GAO Security for access to the AFIS and/or HRMS;
   - Monitoring AFIS and/or HRMS security for the agency;
   - Performing informal reviews of the AFIS and/or HRMS access for the agency on at least a quarterly basis (see paragraph IV.B.8);
   - Performing formal reviews of the AFIS and/or HRMS access within agency on an annual basis (see paragraph IV.B.8);
   - Reviewing and updating Signature Authorization forms (GAO-3) on a regular basis (at least annually);
   - Monitoring the list of WAC holders,
   - Coordinating security issues (with the agency's other Security Administrator if different individual).

5. Supervisors and the Security Administrators shall require their staff to complete any applicable AFIS and/or HRMS training classes prior to requesting access to a system. Additionally, the supervisors and Security Administrators should encourage all current users to complete any applicable AFIS and/or HRMS training classes for appropriate training and update purposes (see paragraph V.C.1., for more information on training).

6. All security update requests must be submitted to the GAO using the appropriate form(s), i.e., GAO-3, GAO-9, GAO-96. Upon completion of the request, the forms remain on file at the GAO.

7. When an employee's status change affects his/her access to any application, the change must be reported to GAO Security immediately using the proper forms. A status change may include a change in position or duties, transfer to another agency, departure from State service, etc.

8. Periodic reviews of all security access should be performed by the agency's AFIS and/or HRMS Security Administrator to ensure that all changes have been documented and security levels are appropriate.

C. Data Sharing Non-Disclosure

1. Policies and procedures relating to Data Sharing Non-Disclosure govern the responsibility of every State employee regarding his/her User ID and information gained using the AFIS, HRMS, or any other financial mainframe system. All users with financial system access are covered by this policy.

2. Each user is required to accept this responsibility by reading and signing the Data Sharing Non-Disclosure form which can be obtained from the agency's AFIS or HRMS Security Administrator.

3. By signing the Data Sharing Non-Disclosure form, the user agrees to refrain from:

- Revealing data to anyone who is not specifically authorized to have the information;
- Attempting to or achieving access to data not applicable to his/her job;
- Entering/changing/erasing data for direct or indirect personal gain or advantage;
- Entering/changing/erasing data in retribution or for personal amusement;
- Using terminals, printers and/or other equipment for non-work related purposes;
- Using another individual's User ID;
- Revealing his/her password or Verification Word to another individual;
- Asking another individual to reveal his/her password or Verification Word.

4. Individuals involved in any of the above are subject to appropriate disciplinary action, up to and including dismissal and/or prosecution in accordance with any applicable provision of law including A.R.S. § 13-2316.

5. The Data Sharing Non-Disclosure form is required to be on file before activating a User ID. Send or fax (542-7066 or 542-5749) the completed form along with the GAO-96 to GAO Security.

6. Individuals with access to another application who have already signed a Data Sharing Non-Disclosure may not be required to do so when requesting AFIS access.

7. See Appendix A for a sample of the Data Sharing Non-Disclosure form.

D. Verification Word

1. The Verification Word policy enables the ISD Help Desk to identify a person who is calling to reset a AFIS/HRMS/LAN password. It also helps to prevent an individual from obtaining another user's password and/or requesting that another user's password be reset.

2. Each user shall obtain a copy of the Verification Word form from the AFIS or HRMS Security Administrator.

3. The user should print his/her name and AFIS or HRMS User ID in the spaces provided.

4. The user should think of a word that can be easily remembered, but not easily associated with him/her. The word cannot be vulgar. This word should not be revealed to anyone, including the user's supervisor or director. The user should write this word on the dashed lines provided. Upon completion of this form, the user shall fax a copy directly to ISD/ISS at 542-0095 and then destroy or mail the original to ISD/ISS.

5. If anyone in the agency requires that the user disclose his/her verification word or any other password, please contact ISD/ISS at 542-2302.

6. ISD/ISS must receive the Verification Word form before activating the User ID.

7. A user needs to complete this form only once for applications security. All future access will use the same word for password reset procedures (see Password Reset for exception).

8. See Appendix B for instructions for completing the Verification Word Form.

E. User ID and Password

1. When a new User ID is established, the user must contact the ISD Help Desk (542-HELP) to activate the new User ID and password.

2. Each employee requiring access to current applications must have his/her own User ID and password. An employee's User ID must not be used by others. In addition, the password must be kept confidential and must not be shared with other employees regardless of the type of access. Failure to do so may result in GAO Security inactivating the release function for the entire agency until proper procedures have been completed by the agency. If sharing of passwords is repetitive, access to the AFIS and/or HRMS will be denied for any function.

3. The user's password will expire every 30 days and the user will be prompted to enter a new password. If the user fails to enter a new password, sign-on capabilities will be

revoked and he/she must contact the ISD Help Desk to have the password reset. (see Password Reset below)

4. If a user has not used his/her User ID in the last 120 days, the User ID will be deleted from the system.

F. Password Reset

1. When a User ID is in 'Revoke' status (prior to activation of a new User ID or if the User ID has expired), call the ISD Help Desk (542-HELP) to reset the password.

2. The ISD Help Desk will ask the user for the Verification Word to establish that he/she is the owner of the User ID.

3. If the user knows the Verification Word, the password will be reset immediately.

4. If the user has forgotten the Verification Word, he/she should contact the agency's AFIS or HRMS Security Administrator. The Security Administrator must then contact the ISD Help Desk.

5. The Security Administrator will be asked to give his/her own Verification Word and will be asked to vouch for the user. The user will then be required to supply ISD/ISS with a new Verification Word.

6. If the Security Administrator cannot supply his/her own Verification Word, the director must request in writing that the password be reset. The Security Administrator and the user will each be asked to supply ISD/ISS with a new, confidential, Verification Word.

G. Signature Authorization

1. The Signature Authorization Form (GAO-3) is used by the agency head to delegate signature authority for various types of documents to responsible individual(s) within the agency. The GAO-3 shall be signed by the agency head and the applicable Security Administrator (AFIS, HRMS, or both).

2. The Signature Authorization Form is required to verify signature authorization on documents sent to the GAO for approval and/or processing.

3. Each agency is responsible for ensuring that all documents sent to the GAO are signed by an authorized signer as indicated on a current GAO-3 on file at the GAO.

4. The applicable Security Administrator (AFIS, HRMS, or both) for each agency should review the Signature Authorization forms whenever an employee changes position or leaves the agency to ensure that the agency's signature authority is appropriate. All Signature Authorization forms should be reviewed and updated on a regular basis (at least annually). This will provide stronger controls on transactions that are approved and/or processed at the GAO.

5. A current update to the GAO-3 should be submitted at least annually by each agency. When a current update is submitted, all prior signatures for the agency or section of the agency will become invalid. This process will enhance internal controls and allow the agency and the GAO to maintain current records.

6. The Signature Authorization Form (GAO-3), or an approved substitute, should be used internally by each agency to verify signature authority within the agency. This will strengthen internal controls on accounting transactions approved and processed by the agency.

7. See Appendix C for detailed instructions for completing the GAO-3.

H. Warrant Authorization Card (WAC)

1. The WAC enables an employee from an agency to pick up warrants at the GAO. The card includes the agency employee's picture, name, agency, eye color, hair color, height, weight, card expiration date and the specific type of warrants the employee is authorized to handle.

   Note: **It is the GAO's policy not to distribute warrants to any employee, with the exception of the agency director, without a valid WAC.**

2. All requests for WACs must be submitted to the GAO using the Warrant Authorization Card Application (GAO-9). The application must be signed by the agency director or his/her designee and the applicable Security Administrator (AFIS, HRMS, or both). It must then be approved by GAO Security and GAO Operations.

3. Upon approval, the GAO notifies the individual who authorized the WAC and schedules an appointment for the employee to have his/her picture taken. WAC pictures are taken at Capitol Police in the basement of the Capitol Executive Tower and the cards are sent to the GAO for distribution.

4. Any cardholder who picks up warrants for another agency must have an agreement on file with GAO Security. It should be signed by the directors of both agencies and should outline the specific details of the agreement.

5. The ability of an employee to pick up vendor warrants should be controlled to ensure that the individual does not also have access to input and release documents, add vendors to the vendor file, and perform financial reviews and reconciliations.

   Employees authorized to pick up payroll warrants should not be able to add an employee to the HRMS system or modify an employee's information.

6. When picking up warrants, the employee should perform a review to ensure that he/she has all warrants for which he/she signed and only those for which he/she signed.

7. Upon receiving the warrants, each agency must have procedures in place to verify that the warrants are made out to the appropriate vendor or employee (for payroll warrants), correct in amount, and properly authorized.

8. Once an employee has been issued a WAC, the card must be kept in his/her possession at all times. Only upon departure from State service or cancellation of the card should the employee relinquish possession of the card.

9. If a WAC is lost or stolen, or a card holder is no longer authorized to pick up warrants, the WAC must be canceled immediately by contacting GAO Security. The WAC should also be retrieved from the employee (whenever possible) cut in half and sent to the GAO with the GAO-9. The form should indicate the reason for cancellation, i.e., change in position or duties, departure from State service.

10. WACs expire one year after the date of issuance. The GAO may authorize continued use via renewal stickers in lieu of issuing a new card.

11. For WAC renewals, follow the same procedure as for issuance of a new card.

12. WAC renewals requests will not be accepted more than two months in advance of the expiration date.

13. Contact GAO Security with questions regarding the WAC process.

14. See Appendix D for detailed instructions for completing the GAO-9.

V. **POLICIES AND PROCEDURES FOR SECURITY REQUESTS**

A. AFIS Security Authorization Form (GAO-96)

1. All AFIS security requests must be submitted to GAO Security using the AFIS Security Authorization Form (GAO-96). Original requests remain on file at the GAO. The form may be faxed (542-7066 or 542-5749) and the original mailed to GAO Security in order to reduce turnaround time.

2. AFIS Security requests may be submitted to add new employees, change existing security levels, delete User Classes, delete User IDs, process DataQuery access requests, or complete any other type of request involving AFIS Application Security.

3. Again, to add, change, or delete a user, send the completed original GAO-96 to GAO Security. If a rush is requested, fax a copy and send the original GAO-96 to GAO Security.

   When adding a new user, the Data Sharing Non-Disclosure may be sent with the GAO-96 to GAO Security. As previously stated, the Word Verification Form must be received by ISD Security and the Data Non-Disclosure form must be received by GAO Security prior to activating the User ID for the new employee.

4. When an employee's status change affects his/her AFIS access needs, the change must be reported immediately to GAO Security using the GAO-96. A status change may include a change in position or duties, transfer to another agency, departure from State service, etc.

5. AFIS security requests for new employees can be made prior to the employee's actual start date by submitting a copy of the GAO-96 without the employee's signature. When the employee begins working, the original GAO-96, with the employee's signature, must then be submitted to GAO Security.

6. Emergency requests require the approval of the agency director or his/her designee on the GAO-96 in addition to verbal approval from the GAO Security group. All forms should specify that the request is urgent and include a corresponding explanation.

7. The AFIS Security Administrator is responsible for formally reviewing the agency's AFIS access on an annual basis. A list of User IDs with current access is provided by the GAO for review. The AFIS Security Administrator is responsible for verifying that the list includes only current employees and that each employee has only the appropriate and necessary access for his/her duties.

   The AFIS Security Administrator should also review the existing internal control procedures when assessing each employee's appropriate and necessary AFIS access.

   The list of User IDs includes a signature line for the AFIS Security Administrator and the agency director to certify their review and approval of all access within the agency. Any necessary changes should be made immediately via a GAO-96 and forwarded to GAO Security. The AFIS Security Administrator should also perform informal reviews at least quarterly.

8. See Appendix E for detailed instructions for completing the GAO-96.

B. AFIS Security Restrictions

1. Edit Mode 2 is not allowed on Deposits, Inter-Agency Transfers, Intra-Agency Transfers and Automated Transfers.

2. Release authority is not allowed on Deposits, Administrative Adjustments, Inter-Agency Transfers, Appropriations and Capital Project Claims.

3. Fund Override on any transaction other than Deposits is granted only with special approval from the State Comptroller.

4. Claims on which the payee is not required to include a vendor number and which bypass the 1099-MISC reporting process (TCs 238, 825, 826, 827, 840, 841) are restricted to the agencies that submit a written request to the GAO for approval. This request should detail the specific situation for which this type of claim is needed. Use is limited to these

approved situations. For internal control purposes, input and release on these claims must be segregated.

C. AFIS Training

1. The GAO Security group **requires** the following AFIS Training:

Prior to receiving access for:	**The user must complete this training course(s) offered by the GAO (AFIS Institute):**
User Class 42 (Intra-agency transfers)	Intra-Agency Transfer & Release *
DataQuery	DataQuery *
Travel Claim Release	Travel Claims/Claim Release *
Vendor File Access	Vendor Set-Up
	* Prerequisite(s) Required

Contact the AFIS Institute Registrar (542-6212) for more information on training courses offered by the GAO, i.e., course descriptions, training schedules, prerequisites.

In the event of time constraints, GAO Security may grant short-term access to the preceding categories. However, users must attend the applicable training classes offered by the AFIS Institute within three months of access being granted. If training has not been completed within the three month grace period, the user's access to the applicable function will be inactivated.

Requests for short-term access must be justified in writing by the agency director or CFO, and will be considered by GAO Security. To expedite the process, a copy of the request may be faxed (542-5749 or 542-7066) and the original sent to GAO Security.

2. In addition, GAO Security recommends that users complete training before obtaining access for or assuming the responsibilities for the following:

- Fixed Asset Data Entry
- Fixed Asset Corrections
- Cost Allocation Profile (screen 22) (see #3 below)
- Recurring Transaction Request (screen 93)
- Security Administrator

3. Specialized training may be provided by the GAO upon agency request. Requests should be submitted, in writing, from the agency head to the State Comptroller.

D. Form Printing

1. The AFIS Form Print program (Screen 56) enables agencies to print Claim and Deposit forms at remotes sites as necessary.

2. Form printing requests must be sent to GAO Security using the GAO-96. ISD must be notified for the initial establishment of the printer(s) that will be used.

3. When requesting form printing capability, the AFIS Security Administrator is required to complete the 'Printer ID' field on the GAO-96. The Printer ID should be four characters in accordance with the established parameters. Contact ISD for the initial setup of a printer ID. Each AFIS Security Administrator should retain a list of all agency Printer IDs. The AFIS Security Administrator must also enter either '1' or '2' in column 8 to indicate the ability of the user to create the original form only or produce duplicate copies, respectively.

4. The ability to produce duplicate copies (print the same claim form more than once) must be restricted and controlled.

5. To maintain proper internal control, only users with authority to release claims should have access to print claim forms. Only users with authority to input deposits should have access to print deposit forms.

6. For more information on AFIS Form Printing, please refer to the AFIS Form Printing Instruction Manual.

VI. **APPENDICES**

Appendices A thru E contain sample copies of the Data Sharing Non-Disclosure, Verification Word, GAO-3, GAO-9 and GAO-96 forms, respectively. The forms included in the appendices are for reference purposes only and are not to be used in lieu of the official GAO forms. All official GAO forms may be requested using an Accounting Form Requisition (GAO-77).

THIS PAGE INTENTIONALLY

LEFT BLANK

APPENDIX A DATA SHARING NON-DISCLOSURE

PROCEDURE: This form is used to document the understanding and acceptance of responsibility of every State employee regarding his/her User ID and information gained using the AFIS, HRMS, or any other financial mainframe system. The form must be read and signed by the employee and on file at the GAO prior to activating the user's User ID.

Note: Individuals with access to another application who have already signed a Data Sharing Non-Disclosure form may not be required to do so when requesting HRMS access.

DATA SHARING NON-DISCLOSURE

I have been made aware and understand that applicable laws, rules and ADOA directives bind all ADOA and non-ADOA personnel who have access. I agree to abide by all applicable laws, rules and ADOA directives, and pledge to refrain from any and all of the following:

1. Revealing data to any person or persons outside or within the agency who have not been specifically authorized to receive such data.
2. Attempting or achieving access to data not germane to my mandated job duties.
3. Entering/altering/erasing data for direct or indirect personal gain or advantage.
4. Entering/altering/erasing data maliciously or in retribution for real or imagined abuse or for personal amusement.
5. Using terminals, printers, and/or other equipment for other than work related purposes.
6. Using another person's personal data access control identifier (USERID) and password.
7. Revealing my personal data access control identifier and/or password to another person.
8. Asking another user to reveal his/her personal data access control identifier and/or password.

Appropriate action will be taken to ensure that applicable federal and state laws, regulations and directives governing confidentiality and security are enforced. A breech of procedures occurring pursuant to this policy or misuse of department property including computer programs, equipment and/or data, may result in disciplinary action including dismissal, and/or prosecution in accordance with any applicable provision of law including Arizona Revised Statutes, Section 13-2316.

My signature below confirms that I accept responsibility for adhering to all applicable laws, rules and ADOA directives. Failure to sign this statement will mean I will not be permitted access to ADOA produced media, computer equipment and software.

My signature below confirms that I accept responsibility for adhering to all applicable laws, rules and ADOA directives. Failure to sign this statement will mean I will not be permitted access to ADOA produced media, computer equipment and software.

Name: _____ USER ID: _____
Print Name

Signature: _____ Date: _____

Agency: _____ Phone: _____

Revised 11/02/2006

APPENDIX B VERIFICATION WORD

PROCEDURE: This form is used to provide ISD/ISS with a **confidential** word, as determined by the user, which will be used to verify the identification of an individual calling to reset a AFIS/HRMS/LAN password. The form must be read and completed by the user and on file at ISD prior to activating the user's User ID.

Note: A user needs to complete this form only once for applications security. All future access will use the same word for password reset procedures.

Employee Verification Word Form

CONFIDENTIAL

Please think of one word easy for you to remember. The word can not be something easily associated to you. The word can not be a vulgar word. This word should not be revealed to anyone, including your supervisor or director.

Verification Word _____
(As an example BLUESKY)

PRINT YOUR NAME: _____

PRINT YOUR USERID: _____

NEW EMPLOYEES: After completing this form fax it and the non-disclosure form to (602) 542-0095.

CURRENT EMPLOYEES: If you want to change your verification word because you believe some one else knows your word, you may submit a new form. We will need your name, USERID and the new verification word to update your records.

The purpose of the verification word is to ensure that when you call the ADOA Help Desk, (602) 364-4444; they will reset your password to your USERID for you and not someone else. When you call, please tell them your name and your USERID. They will enter that USERID and the computer will give them additional information. The Help Desk person will ask you for your verification word. Please say the word you have provided (the one above). They will confirm that information with what they see, and if it matches/correct they will reset the password to your USERID. They will not reset the password if you give them an incorrect word. They will not provide additional guesses, clues or hints.

Last Updated 11.02.2006

APPENDIX C GAO-3

PROCEDURE:

This form is used to evidence Signature Authorization, as designated by the agency head to responsible agency individuals, for all documents that are approved and/or processed at the GAO.

The elements on the form are:

- **CURRENT UPDATE/CANCEL ALL PRIOR** - Mark an "X" in the box, ONLY when submitting a Current Update. A Current Update should be submitted at least annually. **When a Current Update is submitted, all prior signatures for the agency or section of the agency will become invalid.** This process will allow the agency and the GAO to maintain current records.

- **EFFECTIVE DATE** - Enter the date that the signatures will become effective.

- **CANCEL PRIOR AUTHORIZATION DATED: -** To replace a form previously submitted with a new form.

- **AGENCY CODE** - Enter the three digit agency code.

- **AGENCY NAME** - Enter the agency's full name.

- **AGENCY SECTION** - Identify the section, division, unit, or group of the agency for which the authorized signatures are valid.

- **STATUS** - Enter "**D**" for **delete** or "**A**" for **add**. This column is used when the agency is adding an employee for the first time, changing a signature authorization, or deleting an employee's signature authorization. If there is a change in an employee's signature authority, position, or name, delete the previous signature authority and add the new signature authority. For example, if an employee had authority to sign claims, but will now have authority to sign claims and transfers, delete the authority to sign claims and add authority to sign claims and transfers.

- **EMPLOYEE'S NAME & TITLE** - Type or print the employee's full name and title.

- **EMPLOYEE'S SIGNATURE** - The employee must sign his/her full name as it will appear on the authorized document or form. This will be identified as the employee's authorized signature.

  Note: If the employee uses initials to sign documents, both the name and initials must appear on the GAO-3.

- **AUTHORIZED BY** - The name and title of the responsible agency head and applicable Security Administrator (AFIS, HRMS, or both) must be printed or typed. The responsible agency head and applicable Security Administrator(s) must sign his/her name and enter the date signed.

- **AUTHORIZED TO SIGN** - Use the key provided on the form to help enter a complete list of the forms that the employee will be authorized to sign. The list below is not all inclusive, but is intended as a guide to items that require an authorized signature.

-

100 - ALL AFIS (Should be restricted). This should be restricted to those who have responsibility and accountability for all AFIS-related activities of the agency; for example, directors, deputy directors, CFOs, or someone to whom this global responsibility has been delegated.

101 - Administrative Adjustments - Includes claims and transfers.

102 - Appropriation/Allotment Transfers - Includes changes or transfers in appropriations or allotments.

103 - Capital Projects - Includes claims for capital projects.

104 - Claims - Claims other than capital projects and travel.

105 - Deposits - Includes deposits made with the State Treasurer.

106 - Encumbrance/Pre-Encumbrance - Includes encumbrances/pre-encumbrances or purchase orders.

107 - Fixed Assets - Allows of changes to fixed assets and to clear the suspense file.

108 - Out-of-State Travel Request - Out-of-State Travel Requests must be signed by the agency head or designee.

109 - Travel Claims - Authorizes individual to sign travel claims only. This does not give authority for Out-of-State Travel Requests.

110 - Profiles - Includes AFIS PCA, Index and other agency profiles.

111 - Transfers (Inter or Intra) - Includes inter-agency or intra-agency transfers.

112 - Vendor File Update - Includes ability to authorize setup, change and inactivate vendors on the vendor file.

199 - To grant an individual the authority to act as the AFIS Security Administrator.

Other (Please describe) - Identify any other type of AFIS-related document or form that an individual has authority to sign.

200 - ALL HRMS (Should be restricted) - This should be restricted to those who have responsibility and accountability for all HRMS-related activities of the agency; for example, directors, deputy directors, CFOs, payroll managers, or someone to whom this global responsibility has been delegated.

201 - Handwrites - Payroll warrants produced outside of the normal process on a daily basis.

202 - Supplemental Payment Process - Additions to an employee's normal pay.

203 - Time and Attendance - The ability to authorize an employee's work hours, vacations hours, sick hours, etc.

204 - Warrant Cancellation - The ability to authorize the cancellation of a HRMS warrant through the AFIS system.

204 - Direct Deposit Reversal - The ability to authorize the process of retrieving money erroneously deposited into an employee's bank account.

204 - Partially Canceled Warrant - The ability to authorize the process of receiving money back from an employee, in the form of a personal check or cash, that was overpaid.

205 - Buscard - The ability to approve buscard applications.

206 - Start/Change/Stop Direct Deposit - The ability to authorize direct deposit changes.

207 - Change in Leave Balances - Includes changes in Annual, Sick, Compensatory, Military, etc.

208 - Master File Adjustments - Includes adjustments to Retirement, etc.

299 - To grant an individual the authority to act as the HRMS Security Administrator.

Other (Please describe) - Identify any other type of HRMS-related document or form that an individual has authority to sign.

APPENDIX C (cont'd) GAO-3

EXPIRATION DATE:

ARIZONA DEPARTMENT OF ADMINISTRATION
FINANCE DIVISION

SIGNATURE AUTHORIZATION

Current Update Only

EFFECTIVE DATE:

Cancel Prior Authorizations (specify All or Section)

Agency Code	Agency Name	Agency Section (if applicable)

STATUS: The employee(s) whose name, title, and signature appear below are authorized to sign the documents as indicated on this form.

D-Delete A - Add	EMPLOYEE'S NAME & TITLE (Type or print full name & title)	EMPLOYEE'S SIGNATURE (Sign full name & include initials if used)	AUTHORIZED TO SIGN: * (See key below)

AUTHORIZED BY: Must be signed by the responsible agency head (Department, Board or Commission, etc.) and the Security Administrator for the system being authorized.

NAME (Type or print full name)	SIGNATURE (Sign full name in ink)	DATE SIGNED
Agency Head (Required)		
AFIS Security Administrator (Required for AFIS signature authorization)		
HRMS/HRIS Security Administrator (Required for HRMS/HRIS signature authorization)		

* Authorization to Sign Key

199-AFIS Security Administrator Authority		299-HRMS/HRIS Security Administrator Authority	
100-ALL AFIS except 199 (Should be Restricted)		200-ALL HRMS/HRIS except 299 (Should be Restricted)	
101-Administrative Adjustments	108-Out of State Travel Approval	201-Handwrites	205-Buscard
102-Appropriation/Allotment transfers	109-Travel Claims	202-Supplementals	206-Start/Change/Stop Direct Deposit
103-Capital Projects	110-Profiles	203-Time and Attendance	207-Change in Leave Balances
104-Claims	111-Transfers (Inter or Intra)	204-Warrant Cancellation, Direct	208-Master File Adjustments
105-Deposits	112-Vendor file update	Deposit Reversal, Partially	209-Certification and Claim for Personal Services
106-Encumbrance/Pre-Encumbrance	113-Warrant Card (WAC) Approval	Canceled Warrant	210-Warrant Card (WAC) Approval
107-Fixed Assets	114-Warrant Cancel / ACH Reversal		
Other (Please Describe)		Other (Please Describe)	

GAO-3 (revised 10/03) Send original to GAO; retain copy in agency files

APPENDIX D GAO-9

PROCEDURE:

This form is used to request a Warrant Authorization Card (WAC) for an agency employee. There are three sections for the GAO-9: Section A must be completed for all requests; Section B should be completed for new or renewal requests only; Section C should be completed for cancellation requests only.

The elements on the form are:

REQUIRED FOR ALL REQUESTS:

- **TYPE OF REQUEST** - Check the type of request:

  New - To request a new card
  Cancellation - To cancel a card (if the card is lost, stolen, or returned for any reason)
  Renewal - To renew an expired card

- **AGENCY -** Enter the full name of the agency for which the employee will be authorized to pick up warrants.

- **DATE** - Enter the date of the request.

- **EMPLOYEE NAME -** Enter the name of the employee who will be authorized to pick up warrants.

- **AUTHORIZED BY -** The name and title of the responsible agency head and applicable Security Administrator (AFIS, HRMS, or both) must be printed or typed. The responsible agency head and applicable Security Administrator(s) must sign his/her name and enter the date signed.

- **PHONE -** Enter the telephone number of the authorized signer requesting the card.

- **TITLE -** Enter the title of the authorized signer requesting the card.

- **DATE** - Enter the date the request was signed.

REQUIRED FOR NEW/RENEWAL REQUESTS ONLY

- **EYES** - Enter the employee's eye color.

- **HAIR** - Enter the employee's hair color.

- **HT -** Enter the employee's height.

- **WT -** Enter the employee's weight.

- **WARRANT TYPE -** Check the type of warrants the employee is authorized to pick up: **Vendor**, **Payroll,** or **Both**.

- **EMPLOYEE SIGNATURE -** The employee who is being authorized to pick up warrants must sign the form. Signature indicates an agreement to comply with all security policies and procedures related to the distribution of warrants.

REQUIRED FOR CANCELLATION REQUEST ONLY

- **CARD NUMBER -** Enter the number of the card that is being canceled.

- **COMMENTS -** Include an explanation for the cancellation of the card and any other necessary comments.

APPENDIX D (cont'd) GAO-9

WARRANT AUTHORIZATION CARD APPLICATION

ARIZONA DEPARTMENT OF ADMINISTRATION
FINANCE DIVISION - GENERAL ACCOUNTING OFFICE

Type of request: NEW ☐ RENEWAL ☐ CANCELLATION ☐ NAME CHANGE ☐

REQUIRED FOR ALL REQUESTS

Card Number: _____ (Assigned by the General Accounting Office on New Requests)

Agency: _____ Date: _____

Employee Name: _____ AFIS ID: _____ HRMS/HRIS ID: _____
(Please print) (Indicate User ID if applicable or NONE if not applicable)

Authorized by: Must be signed by the Director (or responsible financial officer as designated on form GAO-3) and approved by the Security Administrator.

_____ _____
Name (Please print) Date

_____ _____
Signature Title

Security Administrator: _____ _____ _____
Signature E-mail Phone

REQUIRED FOR NEW/RENEWAL REQUESTS ONLY

Eyes: _____ Hair: _____ Height: _____ Weight: _____

Check appropriate warrant type for request: Vendor: ☐ Payroll: ☐ Both: ☐

Employee Signature: _____
(Signature indicates an agreement to comply with all security policies and procedures related to the distribution of warrants)

REQUIRED FOR CANCELLATION REQUEST ONLY

Reason: (please mark one) ☐ Lost/Stolen ☐ Terminated/Resigned ☐ Other _____

Comments: _____

_____

Note: The agency Security Administrator is responsible to return the employee's Warrant Authorization Card to the GAO upon termination or transfer of employment.

FOR GAO USE ONLY BELOW

GAO Security Approval: _____ Date: _____

GAO Management Approval: _____ Date: _____

Comments/Notes: AFIS: ☐ N/A ☐ Yes _____

HRMS/HRIS: ☐ N/A ☐ Yes _____

Other: _____

APPENDIX E GAO-96

PROCEDURE:

This form will be used to add new employees, change existing security levels, delete User Classes, delete User IDs, process DataQuery access requests or any other type of request dealing with AFIS application security. All employees with AFIS access will automatically have inquiry access to their agency profiles and some statewide profiles. All required fields should be completed to ensure proper authorization is given to the employee. Detailed instructions for the completion of this form are listed below. To add, change, or delete a user, send the original completed form to GAO Security (1700 West Washington, Room 290, Phoenix, AZ 85007) or fax (542-7066 or 542-5749) and send the original form to GAO Security. The shaded boxes on the form are for GAO use only.

The elements on the form are:

- **DATE -** Enter the current date.
- **TEMPORARY DATE RANGE** - Enter the date range over which the request is to be active. Used only if request being made is for a limited time period.
- **DATAQUERY** - Check this box if DataQuery access is being requested.
- **TSO** - Check this box for download ability.
- **TRAINING DATE** - Enter the date training was completed. Required training must be completed prior to receiving access. See paragraph V.C.1., for more information on required training.
- **REGION** - Check the box for the region in which access is required. Enter one region per request [Production, Training (*GAO USE ONLY*), Stage (*GAO USE ONLY*), Test (*GAO USE ONLY*), Install (*GAO USE ONLY*)].
- **F.A.C.A. -** Check this box for the ability to correct Fixed Assets.
- **APPROVAL SIGNATURES** - All proper signatures must be present for the request to be processed. **The signatures of the responsible supervisor and the AFIS Security Administrator are required for all requests.** The only exception being an emergency situation in which only the agency director or deputy director must approve the request.
- **BATCH AGENCY** - Enter the batch agency (same as security agency unless agency has multiple batch agencies) applicable to the request. The batch agency identifies the agency for which the user may input system transactions.
- **RANGE OF AGENCIES** - For agencies using several batch or document agencies, enter the Agency ID range that will be used for the request.

- **SECURITY AGENCY** - Enter the agency for which the user will be performing system functions (agency structure).

- **SECURITY ORG** - Enter the organization code, if any, to which the security access requested will be limited.

- **PRINTER ID** - Enter the printer ID applicable to the request. This field is required for form printing requests only. [This will be the default printer ID on AFIS Screen 56 (Transaction Form Print)].

- **TYPE OF REQUEST (T)** - Enter one type of request per line.

  N - To establish a new User ID security profile.
  A - To add user class(es) to an existing User ID.
  C - To change to an existing User ID security profile.
  D - To delete user class(es) from an existing User ID.
  R - To remove all system access.
  NC - To change the name on a User ID profile for a user who has had a legal name change.

- **NAME OF EMPLOYEE** - Enter the employee's name.

- **USER ID** - Enter the employee's User ID. The User ID must be entered for changes to, or deletions of, an existing employee's security profile. For new requests, this field will be completed by the GAO.

- **EMPLOYEE SIGNATURE** - All requests must be signed by the employee, except in cases where a deletion is requested due to a personnel action. (Requests made in advance for new hires may be faxed to GAO Security without the employee's signature. Originals with the employee's signature must then be sent to GAO Security).

- **SCREEN ID** - For profile maintenance, enter the Screen ID for the profile access being modified.

- **UPDATE TYPE (U)** - Enter the code appropriate for the type of access requested for the Screen ID.

  0 - Inquiry only
  1 - Add & Change
  2 - Add, Change & Delete

- **USER CLASS** - Enter the User Class(es) requested for the employee. If more than one User Class is requested, they may be placed on the same row only if the Accounting Indicator, Release Indicator, Edit Mode and Fund Override Indicator are all the same. If they are not the same, list them on separate rows.

  The available User Classes and corresponding capabilities may be found using the AFIS User Class Profile (Screen D66). Security risk increases as the number of user classes granted to

individual increases. To decrease security risk, request only the user classes necessary for the employee to perform his/her duties.

- **ACCOUNTING INDICATOR (A)** - The Accounting Indicator determines an employee's access to a batch or document agency or range of batch or document agencies. Enter the Accounting Indicator appropriate to the request.

  0 - Inquiry Only.
  1 - Transaction entry and change for security agency.
  2 - Transaction entry and change for range of agencies.
  3 - Not currently used on AFIS.
  4 - GAO USE ONLY (May be given to agencies on a select basis for inter-agency transfers).

- **EDIT MODE INDICATOR (E)** - The Edit Mode Indicator determines whether transactions will be validated and/or processed on-line or in batch processing. Careful consideration should be given to the edit mode that is requested for a user.

  0 - Batch edit and update
  1 - On-line edit and batch update
  2 - On-line edit and on-line update

- **RELEASE INDICATOR (R)** - This field indicates whether the employee will have batch release authority for the User Class indicated. GAO has determined which user classes can perform the release function. An agency can request a more restrictive release level.

  0 - No release
  1 - Release

- **FUND OVERRIDE INDICATOR (F)** - The Fund Override Indicator determines whether an individual can override budgetary and cash controls on financial transactions. <u>This authority is highly restricted and requires prior approval from the State Comptroller.</u>

  Blank - No Fund Override
  1 - Fund Override Allowed

- **VENDOR FILE ACCESS (V)** - This field is used to request access to the Vendor Profile (Screens 5150 and 5200).

  1 - Add
  2 - Add, Change and Delete (<u>GAO USE ONLY</u>)

- **FORM PRINTING (FP)** - This field is used to request the ability to print forms using AFIS Screen 56 (Transaction Form Print).

  1 - View and print
  2 - View, print and duplicate print

NDIX E (cont'd) GAO-96

- **REQUIRED/OPTIONAL FIELDS FOR REQUESTS:**

REQUIRED FIELDS FOR **ALL** REQUESTS:

Date
Region
Type of Request
Approval Signatures
Name of Employee
User ID **
Employee Signature
Batch Agency
Security Agency
Range of Agencies (if applicable)

** User ID will be provided by the GAO for new employees.

REQUIRED FIELDS FOR **USER CLASS ACCESS**:

Batch Agency
Security Agency
User Class
Accounting Indicator
Edit Mode Indicator
Release Indicator

OPTIONAL FIELDS FOR **USER CLASS ACCESS***:*

Security Org
Range of Agencies
Temporary Date Range
Fund Override Indicator

REQUIRED FIELDS FOR **DATAQUERY ACCESS***:*

DataQuery
DataQuery Training Date

REQUIRED FIELDS FOR **PROFILE ACCESS***:*

Screen ID
Update Type

REQUIRED FIELDS FOR **VENDOR ACCESS***:*

Vendor File Access

REQUIRED FIELDS FOR **FORM PRINTING ACCESS** (Screen 56)*:*

Form Printing
Printer ID

APPENDIX E (cont'd) GAO-96

AFIS SECURITY AUTHORIZATION FORM

Date: _____

Region:

☐ Production ☐ Other _____ (Please specify) ☐ Data Query ☐ TSO ☐ Control-D ☐ Vendor File (Inquiry only) ☐ Fixed Asset Correction (DS3: FAS1) ☐ Form Print (specify type): _____ (96B: 560)

APPROVAL SIGNATURES - (Must be on GAO-3 form)

RESPONSIBLE SUPERVISOR: _____ Phone # _____

SECURITY ADMINISTRATOR AND/OR AGENCY HEAD: _____ Phone # _____

BATCH AGENCY: _____

RANGE OF AGENCIES: _____ to _____ to _____

SECURITY AGENCY: _____ _____

SECURITY ORG: _____ _____

If temporary request, effective date range: _____ to _____

1 TYPE	NAME OF EMPLOYEE (Please Print)	USER I.D. (not required for new user request)	EMPLOYEE SIGNATURE	USER CLASS	2 A	E	3 R	4 F	5 DM	6 Screen Access: (full access of add, change and delete given unless otherwise specified)

COMMENTS: _____

GAO USE ONLY

Entered by (initial): _____ DATE: _____

Verified by (initial): _____ DATE: _____

1 TYPE OF REQUEST: N - New User ID; A - add User Class; C - Change User Class; D - Delete User Class
R - Remove All System Access; NC - Name Change

2 ACCOUNTING TRANS (A): 0 - Inquiry Only; 1 - Transaction Entry/Change(Sec Agy); 2 - Transaction Entry/Change (Any Range)
3 - Same as 1 plus change of approved docs (GAO only); 4 - Same as 2 plus change of approved docs (GAO only)

3 BATCH EDIT MODE (E): 0 - Batch Edit/Update; 1 - On-line Edit/Batch Update; 2 - On-Line Edit/Update

4 RELEASE FLAG (R): 0 - No Release; 1 - Release

5 FUND OVERRIDE (F): Blank - No Fund Override; 1 - Fund Override (GAO approval required); 2 - Invoice Validation Override
3 - Both Fund and Invoice Validation Override (GAO only)

6 DISBURSEMENT METHOD (DM): 2 - Required for User Classes where warrants are generated

GAO USE ONLY

WAC _____

Sent _____

AFIS _____

Excel _____

Contacted _____

Change # _____

GAO-96 (revised 10/03)