Chapter 125

Title: Information Systems Access Procedures

I. Applicability

These procedures apply to Authorized DHS Approving Managers (ADAMs) and users attempting to gain access to DHS Information Systems and describe the procedures needed to obtain access.

II. Procedure

(a) All persons requiring access to DHS Information Systems must obtain permission from their divisions' ADAM and be authenticated through the Chief Information Officer's (CIO) designated Systems Administrators. ADAMs and new users must complete and sign DHS Form 359 (for employees) or 5002 (for contractors), "DHS Systems Security Access Request."

(b) Hiring Supervisors are responsible for notifying their division or office's ADAM of a new employee and when an employee leaves or transfers. Hiring supervisors must complete a Form 359 or 5002 and submit to their division or office's ADAM for a change in a user's status (demographic data or type of access, etc.), the termination of a user, and when a user transfers to another location or division. In the case of a transfer, only the user's network account and email transfer. All other access will be based on the new permissions.

(c) By signing DHS Form 359 or 5002, ADAMS certify that:

(1) Access requests are made on behalf of persons who are DHS employees in good standing or non-DHS users who are members of an organization with whom a formal agreement is in place to permit access to DHS systems and safeguard protected information;

(2) Users have provided accurate identifying information and have a legitimate and official purpose for the requested level of access;

(3) Users have been notified of DHS policies pertaining to the appropriate use of state equipment and systems and the safeguarding of private information and that users have completed the required DHS Security and Privacy training; and,

(4) He or she agrees to notify the DHS Systems Security Gateway of material changes in a user's employment status as it relates to the DHS network services or systems applications to which the user has been granted access.

(d) By signing DHS Form 359 or 5002, DHS Information System users certify that he or she:

(1) understands that access to state-furnished equipment, software, and data is restricted to authorized persons only and may be used for official business purposes only;

(2) accepts responsibility for appropriate utilization of state-furnished equipment and understands that computer devices, network activity, email, and internet access may be monitored to detect improper or illicit activity;

(3) has no expectation of privacy in the use of state-furnished computer equipment and services;

(4) agrees to take all necessary measures to safeguard the security of his/her access credentials (username, password, smart card) and is accountable for any unauthorized usage of access credentials that results from his/her negligence or purposeful action; the user agrees to immediately report any compromise of access credentials;

(5) understands it is a violation of state and federal law to use, permit the use of, or fail to safeguard the security of client information in any way that jeopardizes its confidentiality;

(6) is subject to DHS policies pertaining to safeguarding confidential or sensitive information, penalties for inappropriate use of state equipment and electronic communication services, and sanctions for violations of related DHS Conduct Standards; and,

(7) understands penalties for unauthorized access or inappropriate usage, for DHS or non-DHS users, may include discipline and/or prosecution.

III. Integrated Systems Security Gateway

(a) Upon receipt of DHS Form 359 or 5002 from the ADAM, the Security Gateway Administrator will match identity data against validation data sources. DHS users may be contacted by phone and verbally challenged for their AASIS number. The confirmation of other demographic information may be obtained at that time if the Gateway Administrator deems it appropriate. For non-DHS users, the ADAM will be contacted by phone and will be verbally challenged to verify collected information about the user and the request for new user access.

(b) When validation of identity is not successful, the Gateway Administrator will notify the requesting ADAM that the access request was denied. When validation of identity is successful, the Gateway Administrator will re-direct the request to the appropriate Systems Administrators for processing.

IV. User Credentials and Security

(a) Users are assigned a unique personal identifier (username) which must be authenticated in conjunction with a valid password or smart card to gain access to DHS Information Systems. ADAMs should instruct users to safeguard credentials with respect to both physical security and access to DHS Information Systems. The structuring of passwords will meet or exceed prevailing state government standards of at least eight characters with a mixture of alpha, numeric, and special characters.

(b) All Windows or Active Directory based passwords will expire in 60 days and Mainframe based passwords will expire in 90 days, or earlier if changed by user. Users will receive system prompts to change passwords before they expire. Users may not reuse any of their last five passwords for DHS Network access or their last four passwords for Mainframe access. A password should be changed if a user suspects its security has been compromised.

(c) Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but if recorded, the following rules should be observed:

(1) Never openly post User Credentials, particularly in proximity to the user's PC.

(2) Store recording of credentials in a secure location.

(3) Do not identify the recording as a password.

(4) Do not include User Name with password.

(5) Mix in false characters or scramble the password recording in a manner you will remember so the written version is different from the real password.

(6) Never record a password on-line or include it in an email message.

V. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions" and the DHS Employee Discipline policy.

VI. Systems Security Roles Defined

(a) User: A person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any Department of Human Services information system, and who is held accountable for the security of such access. A user may or may not be a Department of Human Services employee.

(b) Department of Human Services User: A person, Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.

(c) Non-Department of Human Services User: A person, not a Department of Human Services employee, who has been granted access to any Department of Human Services information system and is accountable for the security of such access.

(d) System Administrator: Collectively refers to persons exercising the following systems security roles: Security Gateway Administrator, Network Services Administrator, Mainframe Services Administrator, Windows Application Security Administrator, Mainframe Application Security Administrator, Systems Administrators for division supported applications, DHS CIO. The role of such persons is to provide technical support and access management for DHS network services and applications.

(e) Security Gateway Administrator: Persons performing this role serve as the common point of entry for all user access requests. Primary functions include initial evaluation of received access requests, validation of identity, and re-directing of requests for additional processing.

(f) ADAM: Authorized DHS Approving Manager – a class of DHS managers who have been authorized by each division's ADAM administrator to certify user access requests. An ADAM must be a DHS employee. The role of the ADAM is to authorize the submission of security access requests for (1) employees within the manager's division, and (2) non-DHS users affiliated with the manager's division. ADAMs are responsible for the validity of both DHS User and non-DHS User information in all User Access Account records they have authorized (DHS Form 359 or DHS Form 5002, DHS Systems Access Request, available on DHS Share). ADAMs are responsible for notifying the Gateway Administrator of material changes that affect both DHS User and non-DHS User access privileges.

(g) ADAM Administrator: A designee appointed by each division's director to assume the role of managing and maintaining the currency of the division's list of ADAMs. Only those managers appearing in each division's list will be recognized by the Security Gateway Administrator for the purpose of submitting user access requests.

VII. References:

(a) State of Arkansas Policies and Standards
http://www.dis.arkansas.gov/policiesStandards/Pages/default.aspx

(b) State of Arkansas Standard Statement – Data and System Security Classification - Document Number: SS-70-001
http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-001_dataclass_standard.pdf

(c) National Institute of Standards and Technology (NIST) – Computer Security Division – Computer Security Resource Center Special Publications http://csrc.nist.gov/publications/PubsSPs.html

(d) Federal Information Processing Standards Publications (FIPS PUBS) http://itl.nist.gov/fipspubs/

(e) Federal Information Security Management Act of 2002 (FISMA)
http://csrc.nist.gov/groups/SMA/fisma/

(f) Social Security Administration Safeguards (SSA) http://www.ssa.gov/dataexchange/security.html