5001.0.0 INFORMATION SYSTEMS SECURITY ACCESS

5001.0.1 Access to DHS information systems is managed by the DHS Chief Information Officer (CIO), Office of Systems & Technology, by means of an integrated systems security gateway. This policy is applicable to all DHS divisions and offices, and to all DHS information systems.

5001.0.2 All persons requiring access to DHS information systems must obtain permission from their division's authorized DHS approving manager and be authenticated through the CIO's designated Systems Administrators. All users must access DHS information systems through the integrated systems security gateway. DHS network services (including but not limited to Email and Internet), mainframe services, all major DHS applications, all division managed applications and division files shared across the network, must be accessed through the presentation and authentication of network credentials. Access to the Internet through the DHS network, without network authentication, is prohibited.

5001.1.0 Definitions

5001.1.1 Access: Upon the presentation of appropriate credentials, permission to use DHS information systems.

5001.1.2 Authentication: The automated comparison of presented user credentials with credentials on record for access to DHS Information Systems.

5001.1.3 DHS Information Systems: DHS Network services (Network access, Email, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

5001.1.4 Person: For the purposes of this policy, a person is defined as a uniquely identifiable and distinguishable human being, whose identity has been validated and whose association with DHS has been certified by the division requesting access credentials. A person may or may not be a DHS employee.

5001.1.5 Integrated Systems Security Gateway: Common point of entry for all security access requests and authorizations.

5001.1.6 User Access Account: A record, specific to a person and maintained by DHS Network Administrators, containing a user's identifying information and recording types and history of user permissions to DHS information systems. User access accounts must be attributable to an accountable person.

5001.1.7 Generic Access Account: Systems access permissions based on a User Name attributable to a system or business process. Such accounts may exist only on an exception basis, require CIO approval, and must be attributable to an accountable person.

5001.1.8 Credentials: Consists at a minimum of the combination of a user's User Name (or similar user identifier), and Password. Users present credentials, when prompted, to access DHS information systems.

5001.1.9 Validation of Identity: The process of substantiating that users are who they purport to be. User demographic and personnel identification information is received by the Security Gateway Administrator, is compared against validation data sources, and is re-confirmed by challenge-response contact with user.

5001.2.0 Systems Security Roles

5001.2.1 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 DHS information system, and who is held accountable for the security of such access. A user may or may not be a DHS employee.

5001.2.2 DHS User: A person, DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5001.2.3 Non-DHS User: A person, not a DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5001.2.4 System Administrator: For the purpose of this policy, this term 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 Chief Information Officer. The role of such persons is to provide technical support and access management for DHS network services and applications.

5001.2.5 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.

5001.2.6 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, DHS Systems Access Request, available on DHS Gold). ADAMs are responsible for notifying the Gateway Administrator of material changes that affect both DHS User and non-DHS User access privileges.

5001.2.7 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.

5001.3.0 System Security Certification

5001.3.1 ADAM CERTIFICATION: Authorized DHS ADAMs certify by signature on DHS Form 359, the following:

A. That such access requests are made on behalf of persons who are DHS employees in good standing, or if a non-DHS user has been verified to be a member of an organization with whom a formal agreement is in place to permit access to DHS systems and to safeguard protected information;

B. That users have provided accurate identifying information and have a legitimate and official purpose for the requested level of access;

C. That the users have been apprised of DHS policies pertaining to the appropriate use of state equipment and systems services, pertaining to the safeguarding of private information, and have received required HIPAA (Health Information Portability and Accountability Act) privacy training;

D. The ADAM agrees to notify the DHS Systems Security Gateway of material changes in users' employment status as relates to the DHS network services or systems applications to which users have been granted access.

5001.3.2 USER SECURITY AGREEMENT AND CONFIDENTIALITY STATEMENT: Users certify by signature on DHS Form 359, the following:

A. That the user understands access to state-furnished equipment, software, and data is restricted to authorized persons only and may be used for official business purposes only;

B. That the user 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;

C. That the user understands he/she may hold to no expectation of privacy in the use of state-furnished computer equipment and services;

D. That the user understands system credentials allow access to all DHS network services, associated data, and system applications; the user agrees to take all necessary measures to safeguard the security of his/her access credentials; the user agrees not to share passwords nor employ them in a manner that compromises their security; the user understands he/she will be held accountable for any unauthorized usage of access credentials that results from his/her negligence or purposeful action; the user agrees to immediately report to OST any compromise of access credentials;

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

F. That the user understands he/she is subject to DHS policies pertaining to safeguarding of private information, penalties for inappropriate use of state equipment and electronic communication services, and sanctions for violations of related DHS Conduct Standards;

G. That user understands penalties for unauthorized access or inappropriate usage, for DHS or non-DHS users, may include discipline and/or prosecution.

5001.4.0 Integrated Systems Security Gateway

5001.4.1 A division's ADAM must certify each person as requiring and eligible for access to DHS network and application services, utilizing DHS Form 359, DHS Systems Access Request (available on DHS Gold). A DHS Form 359 will be completed and faxed to the Security Gateway Administrator.

5001.4.2 DHS Form 359 collects demographic information necessary to establish user identity, physical location, window of usage, type of access and services required, all in sufficient detail to satisfy basic security and audit requirements. The form provides detailed user instructions concerning appropriate usage and ADAM certification language. The form requires user signature and ADAM signature.

5001.4.3 The initial basis for establishing user identity, for DHS users, is the user's and the ADAM's AASIS Personnel Number. Similarly, for non-DHS users, the initial basis is the user's SSN and the ADAM's AASIS Personnel Number. For DHS users not yet assigned an AASIS Personnel Number, identity may be provisionally established for seven (7) days by providing user's SSN. There is no provisional access for non-DHS users.

5001.4.4 Upon receipt of DHS Form 359, the Security Gateway Administrator will match identity data against validation data sources.

5001.4.5 Where a match exists for DHS users, the user will be contacted by telephone and verbally challenged for AASIS number. Confirmation of other demographic information may be obtained at that time if the Gateway Administrator deems it appropriate.

5001.4.6 Where a match exists for non-DHS users, the ADAM will be contacted by telephone, will be verbally challenged for AASIS number, and will be asked to verify the request.

5001.4.7 Where validation of identity is not successful, the Gateway Administrator will notify the requesting ADAM that the access request is denied. Where validation of identity is successful, the Gateway Administrator will re-direct the request to the appropriate Systems Administrators for processing.

5001.5.0 Systems Security Functions

5001.5.1 Application Access: Access to all applications connected through the DHS network must be processed through the integrated systems security gateway. Divisions may impose additional identification and authentication requirements. Upon re-direct from the Gateway Administrator, such requirements will be managed by the divisions' own Systems Administrators.

5001.5.2 Network Services Access: Access to all DHS network services (to include but not limited to Network access, Email, Internet, etc.) must be processed through the integrated systems security gateway. All users must access DHS network services through the presentation and authentication of network credentials. Access to the Internet through the DHS network, without network authentication, is prohibited.

5001.5.3 Logon Password Problems: Reports of logon password problems may be made directly to the DIS CallCenter, PH: 1-800-435-7989. For Network access password issues, the Gateway Administrator will contact user by telephone, validate identity, and resolve the access issue. For password issues related to applications, following validation of identity, the Gateway Administrator will re-direct the report to the appropriate Systems Administrator. For password issues related to division supported applications, following validation of identity, the Gateway Administrator will re-direct the report to the appropriate division's Systems Administrator.

5001.6.0 User Management

5001.6.1 Access to all DHS network services and applications must be processed through the integrated systems security gateway. User access account requests, and status changes, are submitted on Form DHS-359. This form must be completed in sufficient detail to satisfy basic security requirements and provide a complete audit trail of each user's history of access permissions. User access accounts must be attributable to an accountable person.

5001.6.2 New User: ADAMs may submit requests for New User access. For non-DHS users, access accounts expire after a specified number of days defined by the CIO based on the business requirements of the group; such accounts may be renewed by the division's ADAM Administrator.

5001.6.3 Change User: ADAMs may submit requests for changes of a user's existing demographic data, change of types of access for network services, and changes of types of access for divisions' applications. Users may submit requests, on their own behalf, for changes of demographic data.

5001.6.4 Terminate User: For existing users, ADAMs may submit requests for termination of access. Termination of access will also occur on the basis of AASIS personnel data extracts. For non-DHS users, DHS has no means of checking personnel data, so it is particularly important that ADAMs actively report terminations of systems access. In addition, for non-DHS users access accounts expire after a specified number of days defined by the CIO based on the business requirements of the group.

5001.6.5 Transfers between Location or Divisions: Transfers to another division, or user changes of location, are reported by submitting a Change request. Transferring or relocating DHS users will retain only their network credentials and email access. The receiving ADAM must ensure the Change report indicates (1) change of user's network and applications access privileges for security purposes, (2) change of user's demographic information for access audit purposes, and (3) change of user's division for network cost accountability purposes.

5001.7.0 Originating Section/Department Contact

Office of Systems and Technology
1st Floor Donaghey Plaza North
P.O. Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032