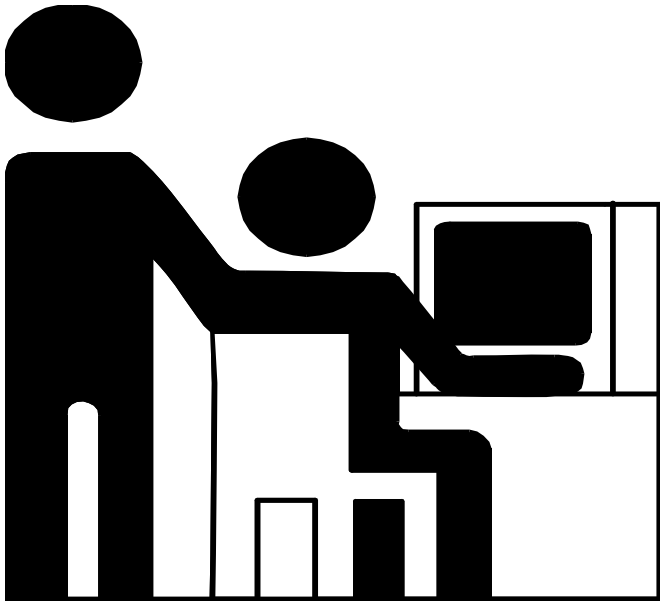
SECURITY DESIGN DOCUMENT

DIVISION OF PUBLIC ASSISTANCE

SYSTEMS OPERATIONS AND NETWORK SERVICES

SECURITY DESIGN DOCUMENT FOR SOLQ

Revised: November 28, 2006



SECURITY DESIGN DOCUMENT

SECURITY DESIGN DOCUMENT

SECURITY DESIGN DOCUMENT

1.0 INTRODUCTION

1.1 DEFINITION

Security is the:

- freedom from exposure to harm, damage, or danger; protection (Webster's Dictionary), and

- protection of data from unauthorized use or intentional destruction. Security measures are typically built into the operation system of a computer and include the checking of passwords, identification numbers and reading and writing privileges associated with each file (Data Management Guide Glossary).

1.2 NEED FOR SECURITY

As the nation experiences a decrease in crime, the incidences of "electronic" crimes, and others of the so-called white collar type crimes, are notable exceptions and continue to rise. Threats to both physical security and communications security exist and are ever present. Electronic fraud continues to grow rapidly.

The definition of felony use of a computer under Alaska Statute Sec. 11.46.740 includes a person who has no right to access (or there is no reasonable ground to believe the person has such a right to access the computer) knowingly accessing a computer or causing the computer to be accessed. As a result of that access, the person obtains information concerning another person or introduces false information with the intent to damage or enhance the data record of a person.

1.3 INDIVIDUAL RESPONSIBILITIES

The potential for a lapse in security of work areas, Eligibility Information System (EIS) access, and safety carries a personal requirement of constant vigilance by all EIS users. The "nothing-has-happened-yet" attitude invites the compromise of communications security, sensitive data handling, and personal safety.

SECURITY DESIGN DOCUMENT

As an EIS user, you have access to confidential client information, proprietary state resources, and proprietary state and federal data. As a state employee, volunteer, or service provider, your **authorized** access to the EIS operating system, any connected subsystem, and the data they provide is a privilege granted by the state to accomplish the job at hand. Authorized access to the EIS is not based on an imagined inherent right. EIS access is granted based upon your trustworthiness, professionalism, and a need to know as it relates to being able to complete the job assigned. Your access to sensitive state database files, and access to sensitive federal files carries your personal obligation to comply with federal and state laws regarding communications security. The security of information, of EIS, and handling client files require you to maintain a constant awareness of and compliance with security guidelines in the daily work routine.

The Systems Operations and Network Services Security Manual is provided to each authorized system user. Each system user is required to maintain the manual and keep it in their work area for review. Supervisors are responsible for ensuring each employee, volunteer and service provider have signed the Division's EIS and Network Services Security Agreement or the Service Provider EIS Security Agreement and read the Systems Operations and Network Services Security Manual.

1.4 CONFIDENTIALITY

The rule making authority of the Department includes the power to establish and enforce reasonable regulations governing the custody, use, and the preservation of the records, paper files, and communications of the Department. Although covered extensively in the Division of Public Assistance's Administrative Manual (including exceptions), the essence of confidentiality is:

> "It is against the law except for purposes directly connected with the administration of assistance programs for a person to solicit, disclose, receive, make use of, or to authorize, or knowingly permit, the use or disclosure of the information obtained from households".

Further reading of the Administrative Manual section regarding confidentiality is essential to your better understanding of applicable Alaska State Statutes requiring the protection of client household information.

The Division of Public Assistance must comply with the data security requirements set forth by other agencies as a pre-condition to the use of their data and/or computer services. The Division's computer services are discussed in the following sections.

SECURITY DESIGN DOCUMENT

1.5 COMPUTER SERVICES OVERVIEW

The Department of Health and Social Services receives its computer services from Enterprise Technology Services (ETS) which functions under the Department of Administration. The Department of Administration carries out its automatic data processing responsibility under Alaska Statute 44.21.150.

The responsibility is carried out through the Alaska Data Center (Juneau) and a data communications network connecting the centers (backup data center in Anchorage) and other agency computing platforms.

Data Security is a function under Agency Support. The Security Administrator helps agencies determine their data security requirements and then assists in the implementation of access controls. The Alaska Data Center assists agencies in maintaining data security through the use of a security software product called ACF2.

Customer Information Control System (CICS) is one of three main accounts available to the customers of the Alaska Data Centers. A CICS account is needed for access to software products on the mainframe computers. The EIS is one of several of the state's major application programs run under CICS. ETS reserves the right to withhold service from customers who are not competent in the software they are using.

1.6 AGENCY RESPONSIBILITIES

Each agency has primary responsibility for security, privacy, and access to their data.

ETS security policy has designated each Department Commissioner as the owner of that Department's data. The data owners themselves must specify appropriate data retention and security requirements. In addition, ETS assigns responsibility for the maintenance of security for data and applications to the customer agency. ETS agrees to act as custodian of that data within the agency designated guidelines.

Each Division Director is advised to designate an official data security contact person for their division through whom all data-security issues flow, and who is responsible for communicating with the Data Security Administrator about such issues. Our Security Officer is the DP Manager II and is located in Systems Operations.

SECURITY DESIGN DOCUMENT

All files maintained by the data centers are considered private and confidential, except for those falling under the Public Information Act. The Alaska Data Center, as custodian of agencies' data, will maintain reasonable safeguards to ensure this confidentiality, and will not release any agency data or files unless specifically requested to do so by the data owner.

All requests for information about an agency's data will be forwarded to the agency for determination of whether the public has the right to the information, pursuant to Alaska Administrative Code Title 6, Chapter 95, Section 010. If the agency determines that the data is public, the agency is responsible for making that data available to the requester. This applies to all material that an agency supplies ETS including but not limited to source data, computer files, reports, listings, and computer programs.

1.7 DIVISION OF PUBLIC ASSISTANCE ACCOUNTS (ACCESS)

In order to gain access (ability to sign on) to EIS, workers must be validated at sign on time by ACF2. To get a CICS account, delete an account, or change an existing account, you must use the LOGONID CHANGE REQUEST form (General Services form number 02-797). If the form is copied be sure both sides of the form are copied.

Two completed forms must accompany each EIS user account request:

- LOGONID CHANGE REQUEST form and
- the signed original of the EIS and NETWORK SECURITY AGREEMENT

  or
- the signed original of the SERVICE PROVIDER EIS SECURITY AGREEMENT.

Comment [RK1]: Need a space here.

A Systems Operations Security Assistant will assign the EIS access profile. The EIS and NETWORK SECURITY AGREEMENT and SERVICE PROVIDER EIS SECURITY AGREEMENT remain on file at Systems Operations and the LOGONID CHANGE FORM is forwarded to ETS in Juneau for further action. A six-character security key is assigned to each person approved to access EIS.

The two forms can be downloaded from the Sys Ops website: http://dpasysops.hss.state.ak.us. (You must use Internet Explorer (IE) to access the website.)

SECURITY DESIGN DOCUMENT

1.8 CHANGES

To change the owner's name of an existing account, use the LOGONID CHANGE REQUEST form and follow directions as for a new account with the following exceptions:

- Check the "CHANGE EXISTING ACCOUNT" square at the top and middle of the form.

- Write the former name in the "OTHER" space below the Data Center list.

1.9 CHANGING ACCOUNT PCNS

To change the state employee account owner's PCN, use the EIS and Network Security Agreement form.

- Check the "Change Existing Account" box in the middle of the bottom of the form.

- Enter personal identifying information and the new PCN

- Submit the completed form to Systems Operations

SECURITY DESIGN DOCUMENT

2. Physical Security

2.1 PERSONNEL ACCESS CONTROLS

Access to State communications, computer equipment, and electronic or printed files within the Division is restricted to those state, contract personnel or volunteers assigned and authorized by the Division.

Managers, supervisors and employees must regularly review their local office procedures for consistency with prudent security methods. Be cautious of procedures that allow total access to all spaces and printed or electronic files. Procedures oriented toward maximum flexibility in response to all office tasks can sometimes be counter to methods limiting control over documents and equipment access.

The challenge to the daily office routine is developing a balance in security procedures that provides a reasonable, cost effective approach, without posing serious obstacles to getting work done. The alternative approach with no controls at all, allowing personnel unlimited access to all areas, can create an office vulnerable to fraud, theft of client information, and unauthorized access to communications equipment.

Methods used for authorized access to work areas or security control options are varied and differ greatly in costs. The more commonly available security options are listed below.

- Key control administration
  - Office space key assignments

- Physical controls
  - Lobbies, desks, counters, limited access signs, etc. which mark and limit outside access to the inner office spaces.
  - Self-closing locked doors
  - Locked Doors

- Personnel Access Controls
  - Establish personnel standards for security access
  - Establish security standards for confidential access

- Non-employee access to work areas either by individual or group requires an employee escort to the office space/employee being visited. The employee visited is required to escort the visitor off the premises upon concluding the visit or interview.

SECURITY DESIGN DOCUMENT

2.2 PRINTED CLIENT FILES

Hard copy prints of client information from EIS data base files are confidential and as such require secure areas for storage and controlled access. Printed EIS client information left on top of desks, filing cabinets, or stacked on floors is subject to compromise.

Anyone having access to printed EIS client information is strictly prohibited from taking the information home. Employee briefcases and other forms of carrying items are subject to being opened by the employee for supervisory scan.

2.3 TRASH DISPOSAL

Inattentive or indiscreet disposal of printed client information from EIS data files or unneeded client documents subjects the client to the potential loss of confidentiality and the potential misuse of proprietary state data.

The use of paper shredding machines to shred printed EIS client information, security key assignments, etc., is a procedural requirement within the Division of Public Assistance. In the absence of on site paper shredding equipment, you may have a contract for shredding confidential documents with a private firm able to guarantee the same level of security and confidentiality required in a DPA office.

2.4 TELEPHONE SECURITY

All telephone switching equipment, servers, HUBs, modems, patch boards, and controller equipment will be maintained in secure rooms with limited access. Rooms containing communications switching equipment will be used exclusively for those purposes and not become multipurpose areas for storing stationary supplies, forms, etc.

Individuals who identify themselves as telephone repair/maintenance personnel must be challenged to show proof of identity and company ID prior to being allowed access to switching rooms. Escort must be provided for personnel who need access for safety and fire inspections.

SECURITY DESIGN DOCUMENT

2.5 PERSONAL COMPUTER (PC) OR TERMINAL SECURITY

State owned or service provider PCs for accessing EIS used by authorized employees and/or service providers must be located in secure areas. Attention to details of access can extend to an EIS work area in an unoccupied office and determining the feasibility of locking the office until an employee is assigned. Employee work or interview office spaces containing PCs must be locked (where possible) upon the absence or departure of the employees for the day.

Common work areas with several PCs present and no controls that limit access to authorized persons only may require special employee procedures in the office.

Anyone unfamiliar to the office work force being observed at a PC must be asked to identify herself or himself and explain their purpose at the computer.

2.6 EQUIPMENT HAZARDS

Electrical and fire hazards in facilities are normally covered by periodic fire and building inspections. In the absence of regular municipal building safety and fire inspections, managers must consider building, fire, and electrical safety as part of their overall security considerations to the equipment in their charge. Type and placement of fire extinguishers must be considered to ensure their suitability for electrical applications. The availability of and access to building fire containment and suppression equipment must be reviewed. Potential water hazards from flooding or fire sprinkler systems on the facility's computer equipment must be included in the office contingency planning.

The impact of high dust environments on equipment and personnel are considerations in facility selections. As a state on the Rim of the Pacific, earthquakes and even volcanic dust need to be part of an office contingency plan. On the presumption there will be some lead time prior to volcanic dust settling down in a DPA office area, supervisors must ensure computer equipment is shut down and covered/wrapped in plastic.

Computer equipment must be protected with surge protectors. Power lapses for as little as one/one hundredth of a second have been known to cause permanent disk damage.

SECURITY DESIGN DOCUMENT

3. System Security

3.1 PASSWORDS

Passwords are used daily as a means of authentication. The password validates your identity and authorization to sign on to EIS. The security key used with a password verifies the menu selections you are allowed. When changes are made to client records, the password and security key determine your identity on the EIS action log.

Keeping your password secret is most important. When someone is using your password and security key, they are impersonating you.

3.2 GENERAL PASSWORD GUIDELINES

EIS users must observe the following guidelines relating to passwords.

- Do not look over someone's shoulder as they are typing in their personal password.

- **NEVER REVEAL YOUR PASSWORD** to anyone.

- Change your password frequently (thirty day standard for log on and network passwords).

- Avoid the use of easily guessed passwords such as: spouses' names, children's names, current month, and popular leisure activities (fishing, skiing, etc., unless misspelled like phishing).

- If a password must be written down, keep it in a locked or secure place.

- Never hesitate to change your password if you suspect that its secrecy has been compromised.

- Notify the EIS Security Officer at Systems Operations immediately via email to the EIS Help Desk (EISHELP@health.state.ak.us - or type EIS Help and hit enter) of personnel terminations, transfers, and name changes. The EIS Security Officer or Assistant will effect the change.

- Shared Logon ID's compromise security and accountability. ETS requires agency data processing managers to obtain unique Logon ID's for each employee who accesses the system.

SECURITY DESIGN DOCUMENT

3.3 CHANGING OR ESTABLISHING ACF2 PASSWORDS

ACF2 passwords are changed on the PRIMARY MENU. (You will hear the Primary Menu called the "Morning Menu" by some EIS users.) You must change your personal password every month. Passwords must be seven to eight characters in length and can be a combination of numbers and alpha characters.

At the bottom of the Primary Menu screen, the EIS user will see the following fields:

Id: _____ PASSWORD: TIME: 10:54:56
LU: CABL NEW PASSWORD: VERIFY: DATE: MM/DD/YY

Enter your assigned Logon ID into the "Id" field. Enter your personal password in the "PASSWORD" field. Passwords must not be less than seven characters long nor more than eight characters. When the password is near its expiration date, an edit message will appear reminding you that your password must be changed.

Password changes require entry into three fields. You must enter your current password along with the new password as follows:

- Enter the current password into the "PASSWORD" field,

- Enter a new personal password into the "NEW PASSWORD" field, and

- Re-enter the new password into the "VERIFY" field, then press the ENTER key. You will access your personal menu screen next, if the new password has been verified.

As shown above, the TIME and DATE readout fields are displayed at the bottom right-hand portion of the Primary Menu screen.

The readout field "LU" (Logical Unit) is located at the bottom left-most portion of the screen. Logical unit is mainframe address. "Terminal ID" is used on an interchangeable basis with logical unit by almost all EIS users. Those using TCP/IP don't get the same LUs each time they log on to the mainframe.

3.4 PASSWORD RESETS

In the event you have forgotten any of your passwords, email the EIS Help Desk (EISHELP@health.state.ak.us) requesting a password reset. Contact Systems Operations with any difficulties in log on or password access.

SECURITY DESIGN DOCUMENT

3.5 SECURITY AUDITS

The Systems Operations Security Assistants conduct security audits of all EIS users statewide throughout the year. A security audit consists of sending new EIS and Network Security Agreements to a designated security contact for everyone in a section. Each person in the section completes a new agreement. The supervisor reviews and signs off on the agreements and they are returned to Systems Operations. The new agreements are compared to the authorized EIS users we have in the section. Any person for whom an agreement is **not** received will be deleted from EIS security. This is also a good time to review the EIS and Network Service Security Manual.

SECURITY DESIGN DOCUMENT

4. Network Services

4.1 INFORMATION TECHNOLOGY GROUP CONNECTIONS

The Information Technology Group (ETS) provides access to EIS, Internet, email and other business critical systems VIA the State of Alaska Wide Area Network (WAN). The network consists of routers, software, telecommunications equipment, and data circuits maintained by ETS and local telephone companies.

4.2 WORKSTATION CONNECTIONS TO MAINFRAME

DPA offices access the Alaska Data Center mainframe through the State of Alaska (WAN). Staff PCs are connected via a CAT 5/5E twisted pair network cable to a network switch, which is connected to a router. The router is connected via DSU/CSU to a commercial data circuit. All State of Alaska offices on the WAN are connected this way. A series of HUB routers in the primary cities are linked together as the WAN core. The Alaska Data Center is located in one of the core sites.

4.3 LOCAL AREA NETWORK (LAN)

A Local Area Network (LAN) is a collection of PCs, printers, servers, and other devices that are connected together in a single location and share resources such as files, disk storage, communications devices, and software. Some common terms are:

- Network Node. A physical device connected to a network. These might include PCs, servers, switches, scanners or printers.

- Workstation. These are PCs on staff's desks.

- Server. A versatile computer that provides multi-user functionality and services and can be set up in a mobile or distributed environment. Examples of services include email, file storage, shared printers, WEB/Intranet, electronic forms, and databases.

- Tape Backup. A tape drive built into a server and used to make a copy of data files that are stored on the server. Some staff may be assigned responsibility to operate the tape backup system for their site.

- Network Drive. Commonly called the K:\ or H:\ drive. It is a virtual container or section on the server hard drive that can be assigned to a user to store files. It's a logical or virtual disk drive as opposed to a physical disk drive. In offices with a server, each staff member connected to a LAN will be assigned a network drive where they can store computer files they create or receive. This is a secure storage location on the network server that is accessible from any location.

- Network Interface Card (NIC). A circuit board card installed in the PC that allows connection of a network cable.

- Uninterrupted Power Supply. A battery backup power supply device intended to protect servers against electrical power line failures.

- Patch Cable. The network cable that connects the PC to the wall jack.

- Switch. A central communications device that allows connections of many workstations to network devices or services.

- Router. A communications device that manages signal traffic within the WAN.

4.4 INTERNET

The Internet is a worldwide network of other networks all connected together by a series of core routers in strategic locations throughout the world. All DPA staff have access to the Internet. The Internet is one of the many business critical systems used by DPA staff. Internet use by DPA staff is subject to the State of Alaska, Department of Health and Social Services and DPA policies for the Use of Technology. There is a great deal of inappropriate material accessible through the Internet. The Department of Health and Social Services has specific training requirements and Internet agreement form to be signed prior to staff accessing the Internet. (Please refer to DHSS P&P 650-2.)

4.5 SPONSORED TERMINALS

Non-state agencies seeking to be connected to the state network must be sponsored by a state agency. ETS charges all costs associated with the installation and annual operation of the network connections to the sponsoring agency.

SECURITY DESIGN DOCUMENT

4.6 INSTALLATIONS OUTSIDE STATE OFFICES

ETS sets forth the following criteria for agencies and individuals outside the state government and for DPA staff that are outstationed in non-State offices to have access to the data network.

- The sponsoring state agency assumes all costs of installation of the network service.

- The non-state entity has physical security limiting access to PCs.

- Password and account security is maintained.

- ETS reserves the right to monitor the activity and data sets of non-state personnel using the ETS data network. This data will be treated as confidential unless there is sufficient evidence that the non-state office is illegally using state computing resources.

-The methods of connectivity to network resources are:

1) Router and data circuit connection to the State of Alaska WAN;
2) Openconnect accounts which provide Internet access to a TN3270 session;
3) Internet provider dial-up accounts that provide PC modem connections to the State of Alaska WAN.

SECURITY DESIGN DOCUMENT

5. SOLQ Security

5.1 GENERAL DESCRIPTION

The Division of Public Assistance implements SOLQ as a Division-wide solution for obtaining client specific information from SSA. To support this initiative, the SOLQ processes are implemented through the Eligibility Information System (EIS). The core systems of the Division have existing interfaces with the EIS related to adding and updating client identifying information. This makes the EIS a good place to implement these interface processes.

The SOLQ interface programs are stored and run on the State of Alaska mainframe. The programs are written in NATURAL and CICS COBOL. The files involved in the SOLQ process are ADABAS files.

5.2 ACCESS

Use of the State Online Query (SOLQ) system is limited to those workers that need this function to adequately perform their duties.

We estimate that there will be **500** workers that will have access to SSA information obtained through the SOLQ interface.

There are three distinct levels of security that a user must pass through prior to being able to access any EIS function.

- Network security.
  - In order to use any of the PC's required to access EIS, the user must logon to the network. The network is a Windows NT network. A unique user ID and password are required. This security is monitored and maintained by the Network Services branch of ETS.
- Mainframe Security
  - The state uses ACF2 to maintain its mainframe security. An ACF2 Logon ID and password are required. ACF2 security is monitored and maintained by ETS.
- EIS Security
  - This is the final level of security a worker must pass through to gain access to the SOLQ interface.
  - The worker is assigned a seven character Security Key. The worker chooses a password and must change the password monthly. This password has few restrictions, but must be no longer than 8 characters.

.

SECURITY DESIGN DOCUMENT

5.3 AUTOMATED AUDIT TRAIL

Every request for SSA information via the SOLQ interface is documented automatically by the system. Each request results in a request record stored in the SOLQ-LOG file. These records are kept as an audit trail and cannot be modified or deleted through any of the Department's automated systems. Access to view the requests is strictly limited and is granted as read-only access to the records. *No SOLQ data is stored on the State system.*

The SOLQ-LOG records contain the following information:

- Action-Type — Was this a normal inquiry on an SSN that exists in EIS? Was this an attempt to inquire on an SSN that does not exist in EIS?
- Action-Date — The date of the inquiry.
- Action-Time — The time of the inquiry.
- Security-Key — The Security-Key of the worker initiating the inquiry.
- Caseload-Num — The number identifying the caseload the EIS client's case is assigned to.
- Unit — The unit the EIS client's case is assigned to.
- FSO — The Full-Service-Office the client's case is assigned to.
- SSN — The SSN used for the request.

To ensure that requests for SSA information are valid requests, the SOLQ interface will only allow inquiries for clients that are known to EIS. All attempts to inquire on clients not known to EIS will be logged and reported.

The SOLQ-LOG file stores the records for at least 3 years. The file is backed up nightly.

Access to the SOLQ-LOG file is restricted to two batch jobs that have read only access.

For reporting purposes, the system can report on activities of individual users or report on requests about any particular SSN. Reports are generated upon request.

Once a week, a report is generated that shows all attempts to inquire on SSN's that are not know to EIS. The Senior EIS Security Officer checks this report weekly.

All potential security problems are reviewed and researched. If a true security violation is detected, it is taken to the user's supervisor, and the supervisor follows up with disciplinary action if necessary.

SECURITY DESIGN DOCUMENT

6. Guidelines

6.1 OFFICE ENVIRONMENT

Management must ensure that adequate security procedures are in place for work areas under their charge. Employees must comply with and maintain the procedures that protect the EIS files, computer resources, and networking devices. This is a team effort. Keeping EIS free from harm requires reminders from one another that our jobs depend on an efficient computer operating system.

The following are your personal responsibilities:

- ✓ You are responsible for the protection of your password and guaranteeing this information is not available to unauthorized persons.
- ✓ Use a different password for accessing networks and the Internet from the password used to access EIS.
- ✓ You are responsible for making only those changes to the EIS client files that you are authorized to make.
- ✓ You are responsible for logging off (backing out to the Primary Menu) the EIS when you are going to be away from within close proximity of your PC.
- ✓ It is your responsibility to report security violations such as unknown persons at a computer terminal with access to EIS to your supervisor.
- ✓ You are responsible for maintaining the privacy and the confidentiality of data you enter into the EIS.
- ✓ You are responsible for securing your work space at the end of the day. This includes the following steps at a minimum:
  - ✓ Log off EIS and computer terminal power off.
  - ✓ Turn off electrical accessories/equipment off (printers, desk lamps, etc.)
  - ✓ Return printed client data back to the appropriate file and the client file back to protected storage.
  - ✓ Close and lock windows (if any).
  - ✓ Lock your personal office door (if available) upon departure.

SECURITY DESIGN DOCUMENT

- ✓ You are responsible for changing your password on a monthly basis. If a password has not been changed by thirty eight days, an edit message (YOUR PASSWORD WILL EXPIRE ON {time/date}) will appear on the screen as you are logging on to EIS.

- ✓ You are responsible for the security of printed client information you receive.

- ✓ Any software obtained from outside state government must be approved by DPA's Network Services prior to installation on state computing equipment.

- ✓ Always make backup copies of your original documents.

6.2 PERSONNEL TURNOVERS

Supervisors must notify the EIS Security Manager via the Help Desk (EISHELP@health.state.ak.us) immediately of any employee termination or resignation. Effective date of EIS access termination must be provided in the notification.

Requests for additional levels of EIS access for persons with new assignments are to be sent with justification to Help Desk by the regional managers or their designees.

6.3 PROHIBITIONS

EIS users and other persons will not cause damage to state computer equipment, operating resources, and data files.

Authorized EIS users will not allow unauthorized persons access to their work station equipment and will not allow those persons to gain unauthorized access to EIS resources and data file.

Do not interfere with any EIS user in the safe and efficient performance of their job by altering their computer equipment or cable connections without their knowledge.

Do not use state computing and communication resources to interfere or disrupt network users, services, or equipment.

It is strictly prohibited to access networks for copying and distributing indecent or obscene material or child pornography when using state computing and communication resources.

Do not use state computing and communication resources to access and distribute computer games that are not related to the agency's mission or training.

SECURITY DESIGN DOCUMENT

Do not seek passwords from or exchange passwords with others.

Do not develop or use programs designed to harass or threaten other users, or inveterate state computers or computing systems, or damage or alter state software components.

Do not use state computing and communication resources or database files for commercial purposes or a personal private business.

Do not send fraudulent computer mail via networks, or break into another's electronic mailbox.

Do not read someone else's electronic mail without their permission.

Do not send fraudulent electronic transmissions such as:

- fraudulent requests for confidential information,
- fraudulent electronic authorizations, and
- fraudulent electronic vouchers or requisitions.

Do not include your password in macros to automatically sign into either EIS or your network account.

Some people delight in finding ways around guidelines and rules. Evading security requirements is not an option in DPA. If you are found to be circumventing system security requirements, you will lose access to EIS and/or the respective network.

6.4 SERVICE PROVIDER ACCESS PRIVILEGES

The Department as owner grants access to its computer, communications and database resources based upon the following factors:

- relevant laws and contractual obligations,
- the service provider's need to know,
- the information's sensitivity,
- risk of damage to the Department, and
- risk of loss by the Department.

SECURITY DESIGN DOCUMENT

The Department as owner reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Service Providers complete and submit the Service Provider EIS Security Agreement to obtain access to EIS.

Access must not violate any Department policies, license agreement, or any federal and state law.

6.5 SECURITY TRAINING AND QUALITY ASSURANCE

New caseworkers will receive an overview in the classroom during system training. Additionally a section in the Administrative Manual, a Broadcast including the EIS procedure and Medelearn (online training) will be in place for current workers as well as new workers upon completion of training. Security will be reinforced continuously with the warning below that will be posted on one of the screens a worker must pass through to obtain the SOLQ information.

WARNING:
Intentional inquiry into a file that is not required
to perform your job or misuse of date obtained
through use of the SOLQ system is a violation of
both State and Federal law and may result in
dismissal and/or felony prosecution
AND
All transactions are monitored.
Do not leave your terminal unattended when logged on.

Quality Assurance will consist of interface checks during case reviews done at the field level by supervisors and at the next level as part of the random selection of cases made by our QA and/or QC departments there will be quality assurance at this level also.

The State of Alaska recognizes and agrees to the need for the SSA to conduct periodic onsite certification and compliance reviews.

SECURITY DESIGN DOCUMENT

6.6 INVESTIGATIONS

Any unauthorized use of your account must be reported immediately to your supervisor.

In the event of evidence that malicious misuse of computing resources has occurred, and if that evidence points to an individual or network, the Department may take the following steps:

- Take appropriate action to protect EIS integrity and user files.
- Notify alleged abuser's supervisor of the investigation.
- Suspend access during investigations of system problems.
- Inspect employee's disks and files if strong evidence exists regarding questionable computing activities.
- Enforcement under the laws and regulations of the State of Alaska will be pursued if appropriate.

SECURITY DESIGN DOCUMENT

7. Organizational Structure

Alaska's Division of Public Assistance is divided into numerous offices around the state.

- **Full Service and Limited Service Offices**
  These offices deal directly with our clients. Eligibility Technicians serve the clients and make determinations as to what Public Assistance programs a client is eligible to receive.
  These offices are located in various communities throughout the State.

- **Field Services**
  The Chief of Field Services is located in *Anchorage* and oversees field operations and services provided in four Regional and 17 local offices statewide. Field Services Unit support staff provides direct support to field staff and collaborates with staff from other agencies and sections on a variety of projects.

- **Policy & Program Development**
  The Policy and Program Development Team is located in *Juneau*. The unit is responsible for developing and maintaining program policy for the Alaska Temporary Assistance (including Work Services and Child Care), Food Stamps, Adult Public Assistance, SeniorCare, General Relief Assistance, Medical Assistance, and Permanent Fund Dividend Hold Harmless Programs. They write administrative rules, policy manuals and forms, answer policy questions, compile statistics and perform program evaluations. They are also responsible for the Division's Work Services grants and contracts.

- **DHSS FMS Information Technology Services (ITS)**
  The Information Technology Services (ITS) Unit is responsible for essential IT functions Department-wide. The Unit provides coordination and oversight for business applications, network services, desktop computer support and telecommunications activities.
    - Business Applications
      The Systems Operations (SYSOPS) Business Applications team provides application development and maintenance support. This team is located in *Anchorage*.
    - Network Services
      The Network Services team provides server related services, such as email, file, print, and network security. This team is located in *Anchorage*.

SECURITY DESIGN DOCUMENT

8. Conclusion

The flow of daily life these days depends on computers running reliably without problems. There are many physical hazards to computer reliability. Potential hazards range from accidental beverage spills to momentary lapse in electrical power. The hazardous journey involved in transferring data places the so-called information society at risk.

Security seems to always focus on willful and malicious activities. Careless actions can be an even larger problem. Financial loss caused by errors and omissions can be more costly than a criminal act.

In the end, everyone who works with computers bears a measure of responsibility for system security. The responsibility can be deciding what measures should be taken, what safeguards to maintain, or simply not to betray them.

STATE OF ALASKA
Department of Health and Social Services
Division of Public Assistance / Systems Operations and Network Services

DIVISION of PUBLIC ASSISTANCE SECURITY AGREEMENT
for
EIS, NETWORK, AND RELATED SYSTEMS

I understand that all client information contained in the Division of Public Assistance EIS database and sources from other agencies via EIS interfaces and Internet providers is confidential. I agree not to disclose any information regarding persons who have applied for, have received, or who are receiving Public Assistance to any unauthorized group or individual; or to any person for any purpose other than the administration of Public Assistance or Medicaid programs.

I will protect all client and/or related information made available to me through interfaces, other agencies, and/or the Internet whether this information is obtained via EIS, direct computer access, hard copy documents, on line viewing, or any other means of communication. This includes, **but is not limited to**, information from the Internal Revenue Service; the Social Security Administration; the Departments of Labor, Revenue and Administration; Public Access Information; and any future information interfaces or Internet services that may be developed.

I understand and agree to comply with the Child Support Enforcement Division (CSED) requirement to protect confidential client information from unauthorized use or intentional destruction.

I understand that I may only use the workstation and Internet access for those specific functions I have been authorized to use.

I understand that my EIS and Network passwords are confidential and may not be kept in written form in unsecured areas. I understand that I am the only one allowed to use my assigned passwords. If I suspect anyone else has knowledge of my passwords, I will report it immediately to my supervisor, the EIS Security Officer, or Network Services. I will change my passwords to EIS and/or the Network at that time.

I understand that whenever I leave my workstation and am not in close proximity, I must sign off from my access to EIS and lock my workstation.

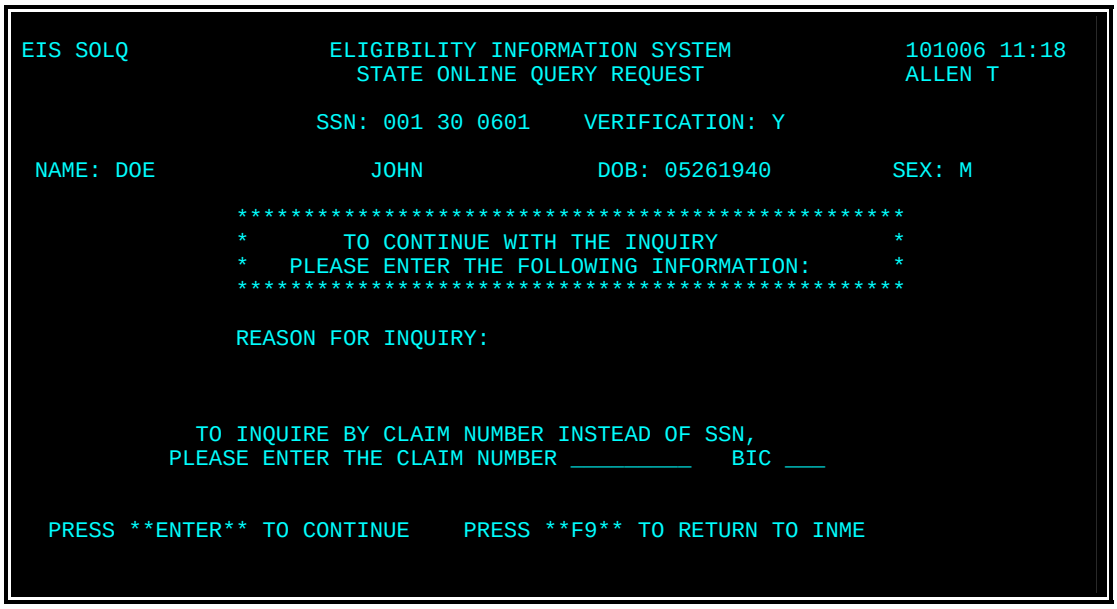
I have read this entire Security Agreement and consent to abide by it. Also, I certify that I have read, understand and will comply with the Systems Operations and Network Services Security Manual, the DHSS Division of Administrative Services Policy and Procedure Manual Section 810, the Use of Department Office Technologies Form, and the State of Alaska ethics policy. Furthermore, I understand that I may be prosecuted if I use EIS or Internet services for fraudulent purposes.

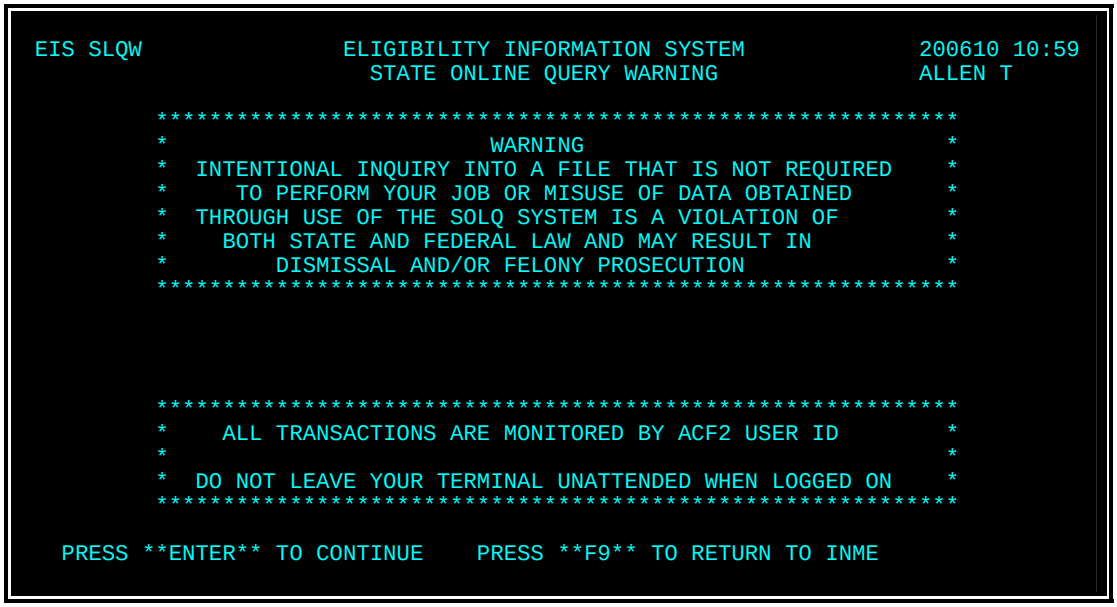
I understand that any violation of this agreement may result in disciplinary action; which may include discharge from duty.

☐ **IVR Prompt Needed**	**Employee (direct line) Phone Number:**		☐ **Network Access Needed** ☐ **PAIS Account Needed**
Employee Name (Print):		**Employee Signature:**	
Job Title:	**PCN:**	**Department:**	**Division:**
City:		**Date:**	
Supervisor Signature:		**Supervisor Title:**	**Date:**

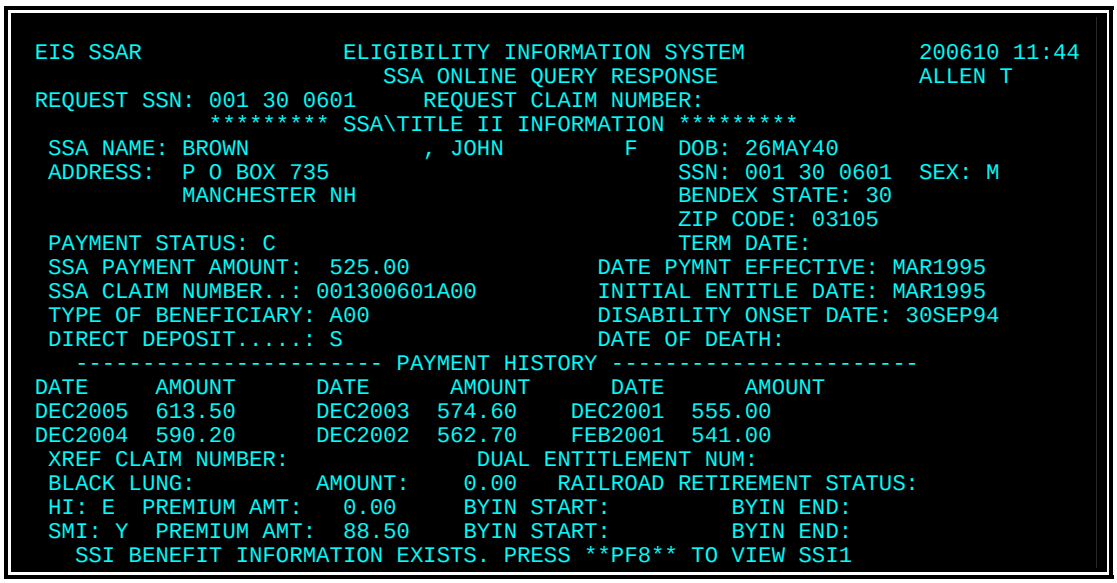
NEW ACCOUNT ☐ **CHANGE EXISTING ACCOUNT** ☐ **DELETE ACCOUNT** ☐

Screen Prints

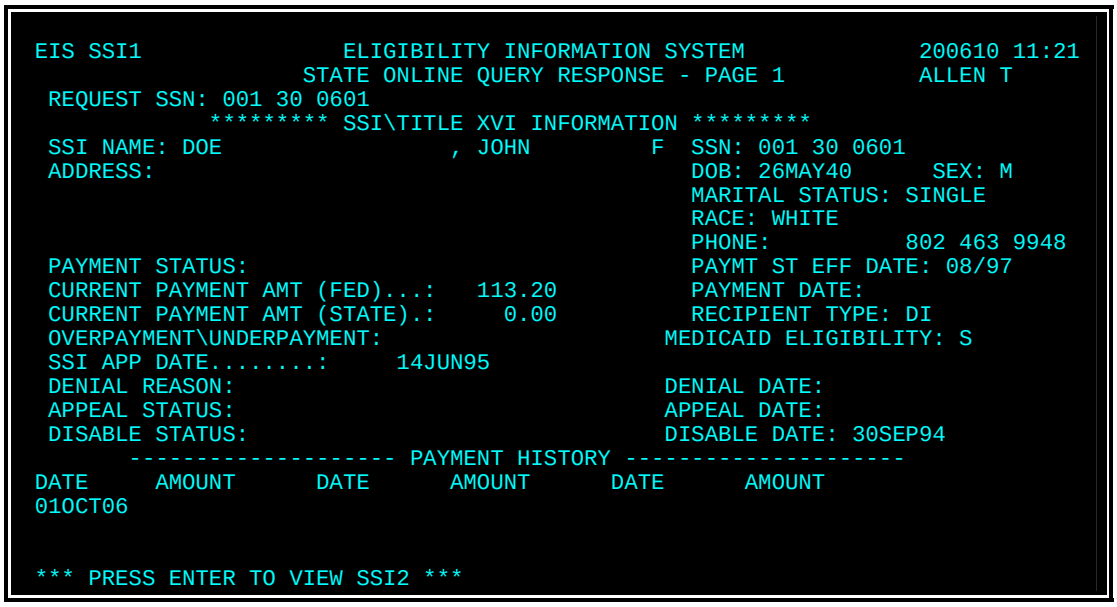


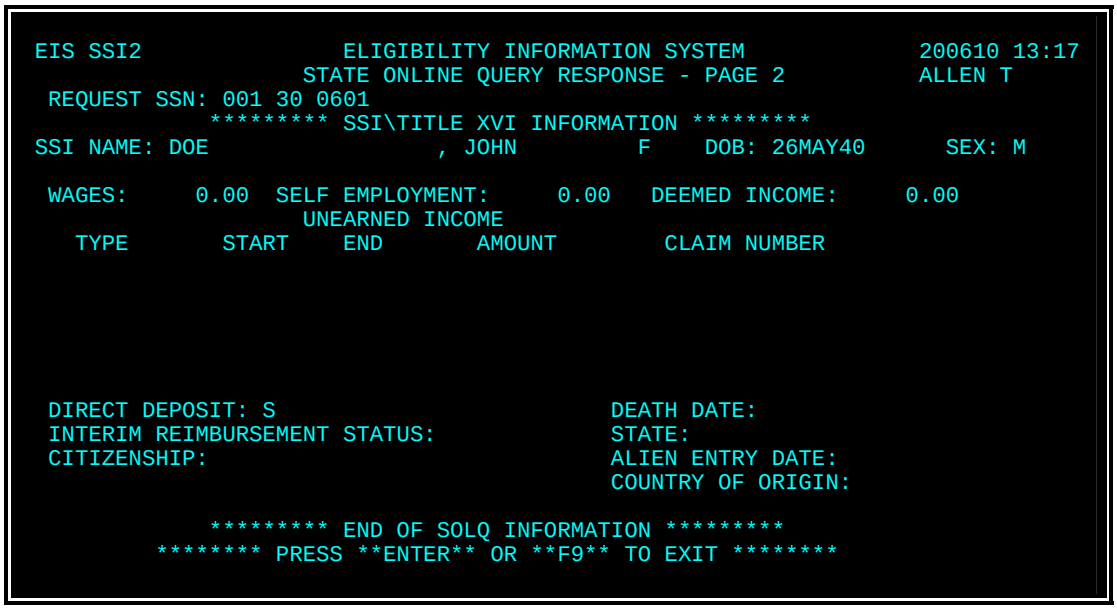


```
EIS SSNR              ELIGIBILITY INFORMATION SYSTEM            200610 11:19
                        STATE ONLINE QUERY RESPONSE             ALLEN T

            ************* REQUEST INFORMATION *************
             SSN: 001 30 0601                  CLAIM NUMBER:
 NAME: DOE                JOHN                 DOB: 26MAY40        SEX:

            ******** SSN VERIFICATION INFORMATION ********

  NUMIDENT SSNS:
   *** MORE INFORMATION HAS BEEN PROVIDED BY SSA ***
   SSA BENEFIT INFORMATION EXISTS. PRESS **ENTER TO VIEW SSAR
   SSI BENEFIT INFORMATION EXISTS. PRESS **PF8** TO VIEW SSI1









                     PRESS **F9** TO RETURN TO INME
```



```
EIS SSAR              ELIGIBILITY INFORMATION SYSTEM            200610 11:44
                        SSA ONLINE QUERY RESPONSE               ALLEN T
REQUEST SSN: 001 30 0601     REQUEST CLAIM NUMBER:
            ********* SSA\TITLE II INFORMATION *********
 SSA NAME: BROWN             , JOHN         F   DOB: 26MAY40
 ADDRESS:  P O BOX 735                          SSN: 001 30 0601  SEX: M
           MANCHESTER NH                        BENDEX STATE: 30
                                                ZIP CODE: 03105
 PAYMENT STATUS: C                              TERM DATE:
 SSA PAYMENT AMOUNT:  525.00              DATE PYMNT EFFECTIVE: MAR1995
 SSA CLAIM NUMBER..: 001300601A00         INITIAL ENTITLE DATE: MAR1995
 TYPE OF BENEFICIARY: A00                 DISABILITY ONSET DATE: 30SEP94
 DIRECT DEPOSIT.....: S                   DATE OF DEATH:
   ----------------------- PAYMENT HISTORY -----------------------
DATE     AMOUNT      DATE      AMOUNT      DATE      AMOUNT
DEC2005  613.50      DEC2003  574.60    DEC2001  555.00
DEC2004  590.20      DEC2002  562.70    FEB2001  541.00
 XREF CLAIM NUMBER:              DUAL ENTITLEMENT NUM:
 BLACK LUNG:         AMOUNT:    0.00   RAILROAD RETIREMENT STATUS:
 HI: E  PREMIUM AMT:   0.00     BYIN START:         BYIN END:
 SMI: Y  PREMIUM AMT:  88.50    BYIN START:         BYIN END:
   SSI BENEFIT INFORMATION EXISTS. PRESS **PF8** TO VIEW SSI1
```


EIS SSI1 ELIGIBILITY INFORMATION SYSTEM 200610 11:21
STATE ONLINE QUERY RESPONSE - PAGE 1 ALLEN T
REQUEST SSN: 001 30 0601
********* SSI\TITLE XVI INFORMATION *********
SSI NAME: DOE , JOHN F SSN: 001 30 0601
ADDRESS: DOB: 26MAY40 SEX: M
MARITAL STATUS: SINGLE
RACE: WHITE
PHONE: 802 463 9948
PAYMENT STATUS: PAYMT ST EFF DATE: 08/97
CURRENT PAYMENT AMT (FED)...: 113.20 PAYMENT DATE:
CURRENT PAYMENT AMT (STATE).: 0.00 RECIPIENT TYPE: DI
OVERPAYMENT\UNDERPAYMENT: MEDICAID ELIGIBILITY: S
SSI APP DATE.....: 14JUN95
DENIAL REASON: DENIAL DATE:
APPEAL STATUS: APPEAL DATE:
DISABLE STATUS: DISABLE DATE: 30SEP94
---------- PAYMENT HISTORY ----------
DATE AMOUNT DATE AMOUNT DATE AMOUNT
01OCT06
*** PRESS ENTER TO VIEW SSI2 ***


EIS SSI2 ELIGIBILITY INFORMATION SYSTEM 200610 13:17
STATE ONLINE QUERY RESPONSE - PAGE 2 ALLEN T
REQUEST SSN: 001 30 0601
********* SSI\TITLE XVI INFORMATION *********
SSI NAME: DOE , JOHN F DOB: 26MAY40 SEX: M
WAGES: 0.00 SELF EMPLOYMENT: 0.00 DEEMED INCOME: 0.00
UNEARNED INCOME
TYPE START END AMOUNT CLAIM NUMBER
DIRECT DEPOSIT: S DEATH DATE:
INTERIM REIMBURSEMENT STATUS: STATE:
CITIZENSHIP: ALIEN ENTRY DATE:
COUNTRY OF ORIGIN:
********* END OF SOLQ INFORMATION *********
******** PRESS **ENTER** OR **F9** TO EXIT ********

SECURITY DESIGN DOCUMENT FOR SOLQ is Approved by:

Paul Schoenborn
EIS Systems Security Officer

Date _____