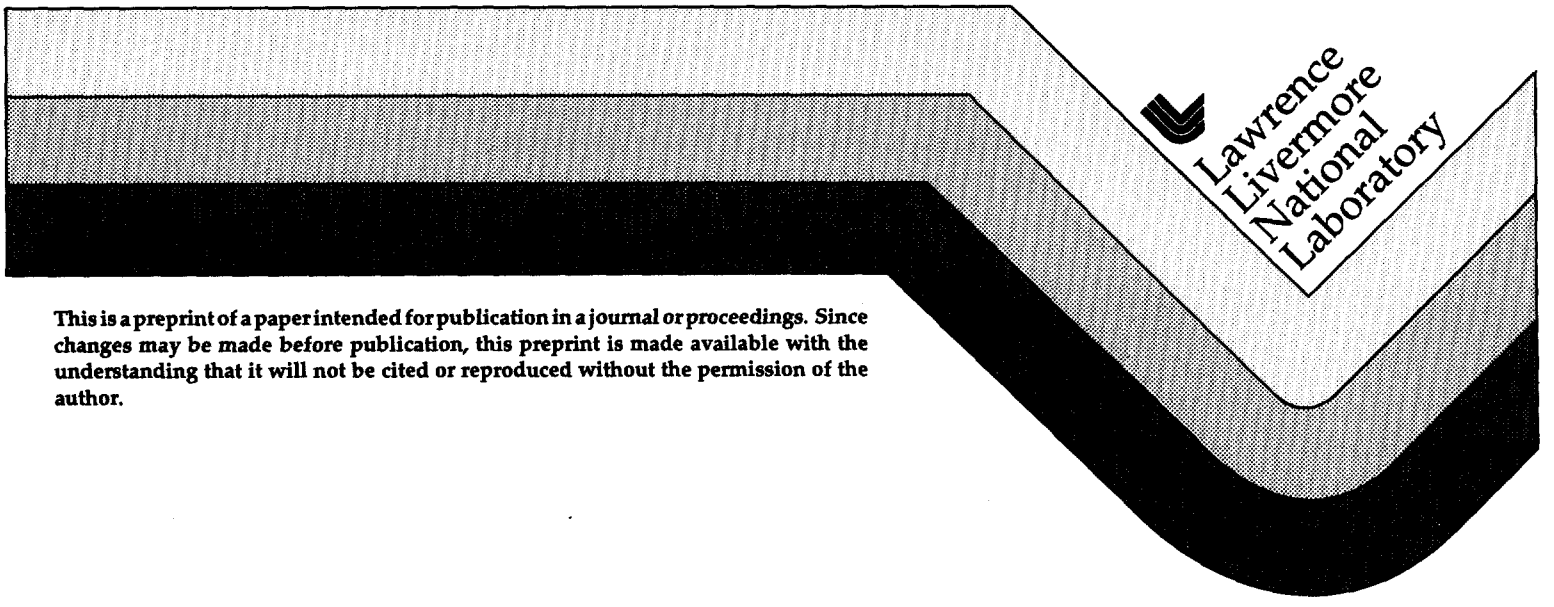
UCRL-JC-126230
PREPRINT

DOE Integrated Safeguards and Security (DISS) System A Nation-Wide Distributed Information System for Personnel Security

B. Block

This paper was prepared for submittal to the
13th American Defense Preparedness Association Symposium & Exhibition
on Security Technology
Virginia Beach, Virginia
June 9-12, 1997

June 5, 1997



DOE Integrated Safeguards and Security (DISS) System A Nation-Wide Distributed Information System for Personnel Security

Bob Block
Security and Automation Technology
Lawrence Livermore National Laboratory
Livermore, CA 94551-0808

Abstract

DISS uses secure client-server and relational database technology across open networks to address the problems of security clearance request processing and tracking of security clearances for the Department of Energy. The system supports the entire process from data entry by the prospective clearance holders through tracking of all DOE clearances, and use of standard DOE badges in automated access control systems throughout the DOE complex.

The Need For Automation

The Department of Energy maintains several hundred thousand active security clearances, and processes tens of thousands of new clearance requests and reinvestigation requests annually. Processing and information needs for this data is nation-wide.

Support for this activity and data was developed when significantly less automation technology was available, and is a combination of considerable manual processing, a variety of old, non-integrated computer systems, local partial databases, cumbersome dialup queries, and uncoordinated, redundant data.

In 1994, the DOE Office of Safeguards and Security commissioned Lawrence Livermore National Laboratory to build a replacement of this combination of older computer systems and manual processing with an integrated, state-of-the-art system that utilized current database, client-server, and security technology.

The resultant system, DISS (Department of Energy Safeguards and Security system) today is almost fully deployed and in the early phases of use throughout the DOE complex.

DISS Overview

DISS conveniently partitions into two major sub-systems: DISS/ET (Electronic Transmission) responsible for processing of security clearance requests, and DISS/PSDB (Personnel Security Database) responsible for clearance tracking and all related information queries.

DISS/ET - Security Clearance Request Processing

The DOE requires that applicants for security clearances and clearance holders needing periodic reinvestigation submit a package of information including a fully completed and signed Questionnaire for National Security Positions (Form SF-86) containing personal history for the number of years required by the level of clearance, a variety of ancillary documents, depending on answers to the SF-86 questions, and, possibly, a classifiable set of the applicant's fingerprints.

For DOE contractor personnel, the process is usually initiated by the responsible DOE prime contractor's Clearance Office. The data is submitted to the Clearance Office by the individual. The Clearance Office reviews the data, collects necessary fingerprints and documents, and works with the individual to complete and correct the data. This package is passed on to the responsible DOE Operations Office with a clearance justification.

For DOE employees, the data and clearance justification go directly to the responsible Operations Office, which in the same manner as the contractor Clearance Office, works with the individual to make the data complete and correct.

For all requests, when the Operations Office is satisfied with the data and the clearance request justification, the request is sent to the Office of Personnel Management's Information Processing Center in Boyers, PA for the required background investigation. The OPM's investigation is outside the scope of DISS. The OPM performs the investigation and returns its findings to the Operations Office which then adjudicates the case. The clearance is either granted or the case enters an extensive administrative review process. with denial of clearance ultimately determined by the Office of Safeguards and Security at DOE HQ.

There are more than forty prime contractor clearance offices, and twelve DOE Operations Offices processing clearance requests. The contractors are located throughout the U.S., with the responsible Operations Offices usually, but not always, located in close proximity. A variety of local automation tools have been in place at the various offices to support portions of this process, but complete automation required a DOE complex-wide effort in the form of DISS/ET.

DISS/ET currently automates the process up to and including communication of the data to the OPM. Future releases are intended to support the return of investigation results to the Operations Offices and adjudication.

Clearance request data is entered and reviewed using a set of PC based client-server applications supplied to the Clearance Offices, the Operations Offices , and the individual applicants. The data is collected and stored in Regional Personal Security (RPS) databases located at the Operations Offices, and on a gateway computer located at the OPM's Boyers, PA facility.

The appropriate data is keyboarded into the responsible RPS via the PC based clients. Ancillary documents are scanned and stored as images in the RPS, again through a PC client. Workflow control and review applications support the processing of cases at both the contractor Clearance Office and the Operations Office. Data for clearance requests ready for background investigation is electronically transferred to the OPM.

DISS/PSDB - Security Clearance Tracking and Information

PSDB is concerned with clearance status and tracking (as opposed to clearance request tracking) and with providing information to the various DOE controlled sites regarding levels of clearance held by local personnel and visitors to their sites. Tracking of clearances begins with the return of background investigation results from OPM to the responsible Operations Office. PSDB retains data on personnel with active clearances throughout the life of the clearance, and for ten years thereafter. Data includes status and level of clearance for all DOE granted clearances, and

history of the clearances held by each individual. The data is maintained in a Personnel Security Database at DOE HQ, referred to as the PSDB.

Beyond the clearance status information, the PSDB also includes badge status and information for DOE standard badge holders from participating sites. For the most part, all the badge data in the PSDB is for DOE personnel with active clearances. It is possible to store badge data for non-cleared DOE standard badge holders.

The PSDB has a third, somewhat unrelated, component. It contains weapons data access authorizations granted for DOE personnel from non-weapons sites, and for non-DOE personnel needing access to DOE weapons data.

Clearance data is entered from authorized PC based clients throughout the DOE complex, and is accessible at a variety of privilege levels to users throughout the complex via PC based and Web based clients.

Badge and related data is supplied to PSDB from stand-alone PC based clients, and from the Argus physical security system used at several of the DOE sites (Argus is the DOE's standard physical security system). This interface allows a Q or L cleared visitor who's badge is enrolled in VADB to gain access to limited areas through automated access controlled portals at participating sites. This is DOE complex wide access control with one badge per individual.

DISS Detailed Description

DISS/ET - Details

Returning now to the clearance request processing, following is a bit more detail.

The SF-86 is the required form for security clearance requests throughout the federal government, and is the mother of all forms. It is large, complex, and unpredictable in ultimate length, since many of the sections require all instances of historical data for a particular date range (5-10 years). Applicants with many residences, jobs, schools, aliases, marriages, etc. will run out of space on the paper form and be forced into use of continuation pages.

The electronic version of the SF-86, "stretches" the form as needed for historical data. This is accomplished by extendible, scrolling sub-sections on the data entry and review screens. Also, since data is typically accessed in a non-linear fashion, the electronic form supports rapid call up the desired section.

A major feature of DISS/ET is to allow direct entry of the SF-86 data by an applicant, from hisor her desk-top computer. To support this, the applicant is supplied with a set of diskettes that will install the data entry application onto a PC running Windows, Windows 95, or Windows NT (a Macintosh version is under development). If this is a reinvestigation with prior data already stored in the RPS, the diskette set also includes the previous data entry, and the applicant need only augment the data with recent history.

The software is self installing. The user types a simple entry phrase, and the DISS/ET applicant entry software installs on the PC. To use the direct entry software, the applicant must have enough computer skill to type and use scroll bars and a mouse. i.e., be a normal PC user.

The applicant entry software includes a Validator that reviews the data for consistency and reasonableness, presenting the applicant with a list of diagnostic messages for each identified discrepancy. Validation takes well under a minute.

As this is sensitive personal data, authentication is required to establish that the applicant is the person who entered the data. To authenticate the entry, the applicant can digitally sign the entered data. This is an RSA public key based digital signature, and is accomplished with a screen button option and entry of the applicant's password, created when the applicant was given the diskette set. If the applicant has access to the internet, the digitally signed document can be e-mailed to the RPS using Privacy Enhanced Mail (again triggered by clicking on a screen button). If not, the data diskette can be postal mailed or delivered to the responsible office.

For applicants without access to a personal computer, or without sufficient computer skills, the Clearance Office or Operations Office staff can enter the data from paper copy.

ET provides complete workflow control and review software to allow routing of the case to various personnel in each reviewing office, as well as routing between the Clearance Office and the Operations Office. ET software retains flexibility so that individual offices can control the workflow as they wish.

Included with the data entry and correction software is the Validator, providing the reviewer the same level of diagnostics as the applicant. As corrections are made, validation can be rerun until the reviewer is satisfied with the data. All changes made to the data are retained in an audit log, so that original entry and change of data can be fully traced by time of entry and user.

Some offices elect to print a copy of the form and have the applicant sign the final copy. Unlike the paper form SF-86, the printed copy stretches the form as needed to sequentially list all data. While data is in the same sequence as the paper form, it does not look like the paper form.

Scanning software is provided at these offices to scan in required documents and associate them with the case. The ultimate goal is to also scan fingerprints, but low cost scanning software and hardware is not yet available that provides the resolution needed for reliable reproduction of the prints to FBI standards.

When the Operations Office is satisfied with the completeness and accuracy of the entered data and scanned documents, the final reviewer transmits the case to the gateway computer at the OPM center. OPM operators can then upload the case data into their computers for further processing. Scanned documents are printed at the OPM center.

Future versions of the system anticipate electronic return of investigation results to the responsible Operations Office, and support of the adjudication process.

DISS/PSDB - Details
PSDB tracks clearance status from the point where investigation results are received from the OPM, through granting or denial of a clearance, and through any subsequent change in clearance status. PSDB also maintains badge and access control information for DOE standard badge holders from participating sites (participation is not mandatory).

Clearance tracking allows authorized users at the responsible Operations Offices to create and modify individual clearance records with the correct clearance and clearance status for all holders of DOE clearances. This is done from PC based client applications to the PSDB server. Similarly, weapons data access requests for non-DOE personnel and DOE personnel from non-weapons sites are entered into the PSDB by authorized users from PC based clients. The data includes dates, sites, and the level of data for which the visitor is authorized access.

Badge holder information can be loaded into the PSDB from any authorized source that has the data. This includes access control systems at the various DOE sites, and stand alone applications. Currently, the Argus physical security system and one PC based client are the available badge data interfaces.

Through secure web page access, sites can determine at a glance the clearance status of any local employee, contractor, or arriving visitor,. Similarly, the sites can determine what weapons data access has been granted to arriving non-DOE visitors or visitors from non-Weapons DOE sites.

PSDB is currently being enhanced to include badge holders' badge photos, for reliable verification of arriving visitors, or persons with lost or forgotten badges. The photos will be compressed and uploaded into the database from PC based clients, and accessible from these clients and the web pages.

For DOE sites with PSDB connectivity to their automated access control system (ACS), the ACS can directly query the PSDB. A cleared DOE visitor with DOE standard badge and access control information maintained in the PSDB can arrive at a visiting site and go directly to an automated access control portal or booth. The visitor enters badge, PIN and biometric, as required by the local system. If the visitor is not found in the local database, the ACS queries the PSDB, finds the visitor's clearance and badge related data. If the visitor presents an active badge, valid PIN, and biometric, as required by the ACS, the ACS can allow access through the portal based on site local policy.

This complex-wide access eliminates multiple badges and associated costs, and increases the security provided for visitor access.

PSDB is in the final stages of user acceptance testing.

DISS Security
DISS processes unclassified, sensitive data over open networks. The security is designed for this environment.

Database Security
All databases are fully firewalled, restricting traffic to only the DISS application, and restricting connections to authorized IP addresses. User accounts are password protected. Each account is provided a role sufficient to perform its authorized tasks. The OPM gateway and each RPS maintains a certificate hierarchy and certificate revocation list for sending and receiving privacy enhanced mail.

Network Security
There are four separate DISS data streams traveling the networks: RPS to OPM communication, applicant e-mail to RPS, PC client to RPS and PSDB databases, and web client to PSDB database.

RPS to OPM communication and applicant e-mail use privacy enhanced mail (PEM). PEM involves DES encryption of the actual message data, RSA public key cryptography for encryption of a one-time DES key, and message digest comparison for authentication of the message originator.

PC and web clients use DES encrypted communication with login to password protected database accounts.

Summary
DISS supports security clearance request processing and security clearance tracking and information for the DOE. The techniques used are as close to state-of-the-art as development and testing of production quality applications will allow, putting the DOE at the forefront of information technology. Significant attention was given to developing intuitive graphic user interfaces, and to insuring security on an open network environment.

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Technical Information Department • **Lawrence Livermore National Laboratory**
University of California • Livermore, California 94551