CONF-960767--24

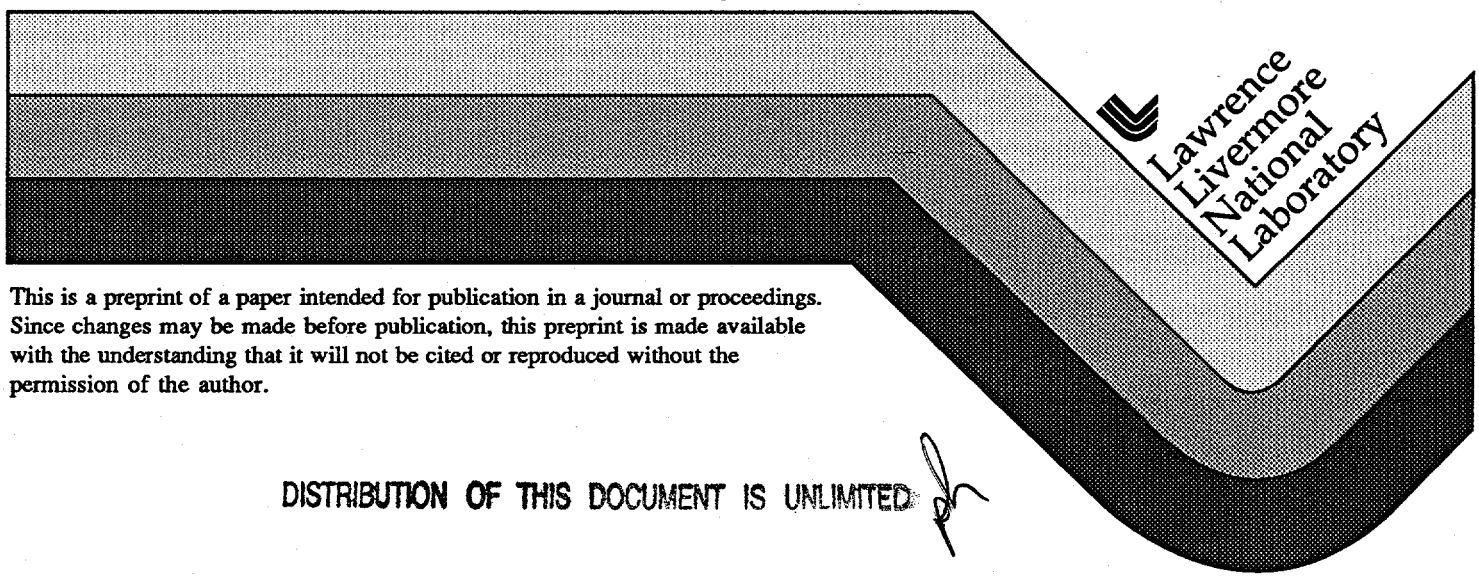
UCRL-JC-124698

DOE's Nation-wide System for Access Control Can Solve Problems for the Federal Government

S. Callahan
D. Toms
G. Davis
D. Johnson
S. Strait

This paper was prepared for submittal to the
37th Annual Meeting of the Institute of Nuclear Materials Management
Naples, FL
July 28-August 2, 1996

July 1996



DOE's NATION-WIDE SYSTEM FOR ACCESS CONTROL CAN SOLVE PROBLEMS FOR THE FEDERAL GOVERNMENT

Samuel Callahan & Darryl Toms
U.S. Department of Energy, NN-51
Germantown, MD 20874

Gregory Davis, Daniel Johnson, & Scott Strait
Lawrence Livermore National Laboratory,
Livermore, CA 94551

Abstract

The U.S. Department of Energy's (DOE's) ongoing efforts to improve its physical and personnel security systems while reducing its costs, provide a model for federal government visitor processing. Through the careful use of standardized badges, computer databases, and networks of automated access control systems, the DOE is increasing the security associated with travel throughout the DOE complex, and at the same time, eliminating paperwork, special badging, and visitor delays. The DOE is also improving badge accountability, personnel identification assurance, and access authorization timeliness and accuracy. Like the federal government, the DOE has dozens of geographically dispersed locations run by many different contractors operating a wide-range of security systems. The DOE has overcome these obstacles by providing data format standards (e.g., for magnetic stripe badges); a complex-wide virtual network for security (DOE Integrated Safeguards and Security or DISS); the adoption of a standard high security system (Argus); and an open-systems-compatible link for any automated access control system. If the location's level of security requires it, positive visitor identification is accomplished by personal identification number (PIN) and/or by biometrics. At sites with automated access control systems, this positive identification is integrated into the portals.

Background

Many of the access control challenges addressed by the DOE are similar to problems facing other agencies in the federal government, and in fact the federal government as a whole. This paper will provide an overview of conditions that led to DOE's new Complex-Wide Access Control (CWAC) system and a brief description of that system. We will leave it to the reader to draw parallels to their own systems and determine the applicability to their venue. The DOE's security requirements are quite high, but because of a graded approach and extensive automation, these solutions adopted for the DOE can be applied to most agencies.

The Department of Energy is a nation-wide complex of facilities and people, working with information and materials whose loss would have a significant impact on national security (Figure 1). Most of the larger facilities are part of the nuclear weapons design and production complex. Controlling access to these facilities and their contents has been, and always will be, critical to protecting public safety, employee safety, and national security. At present, there are approximately 150,000 cleared individuals within the DOE, and many more without clearances badged to work at DOE facilities. There are 13 major facilities with more than 5,000 employees at each. There are frequent site-to-site visits.

In the past each DOE facility developed and implemented its own site-specific access control solution. Since the various badge and system designs were incompatible, an individual traveling from one DOE facility to another DOE facility often had problems gaining access to the intended destination. As intersite visits increased and security awareness grew, this became a noticeable problem.

In response, the Department developed a new concept for access control that spanned the DOE complex. The concept encompassed standardization and automation enhancements in personnel security, physical security, and in security policy, with the goals of making good security transparent to the authorized individual, reducing costs, and building flexibility into the system to ensure consistent and secure operation into the 21st century.

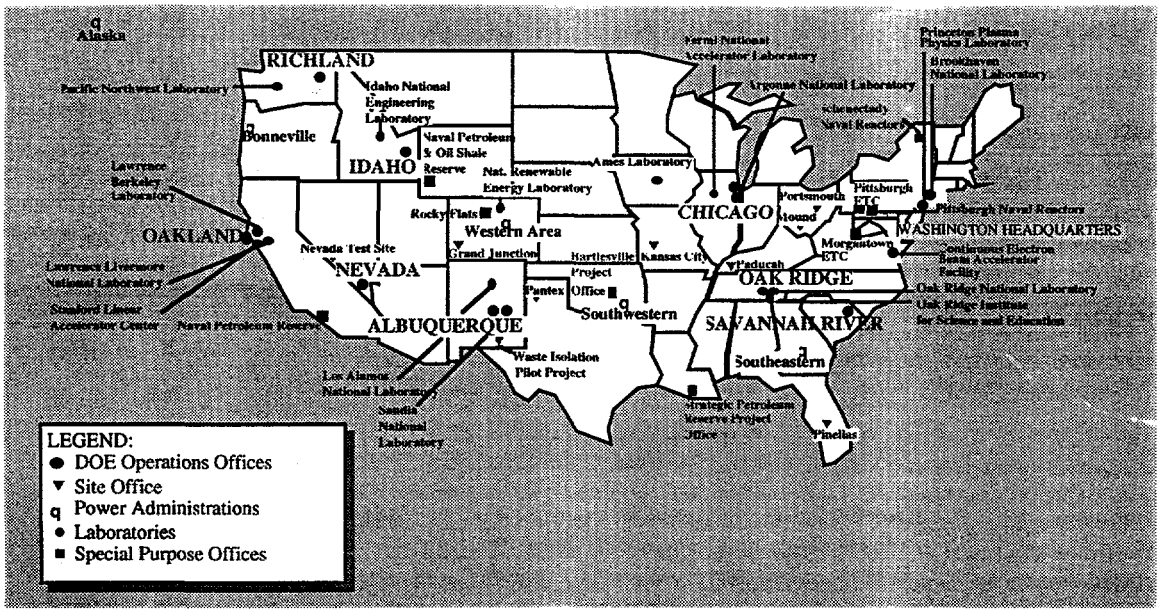


Figure 1. The DOE is a large nation-wide complex with significant National Security interests.

Access Control Problems

Throughout the 1980's and early 1990's, classified visits within the DOE were sometimes difficult, and the cost of supporting the growing number of visits high. Classified visits are those involving travel from one site to another where discussions about, or access to, classified information is required. Paperwork was required at both the origination and destination organizations. The complex process and forms all too often resulted in an authorized individual(s) being delayed or denied access to a site for hours or days. The root causes of the problem were in three major areas: verifying clearance, incompatible badges and access control systems, and communication of special access authorization.

Verification of an individual's clearance

Neither the policy, the technology, nor the infrastructure were in place to allow automated verification of DOE employees or contractors away from their home sites. This generated the need for a set of procedures and paperwork to enable the communication of verification information from one site to another.

The old security forms required many signatures and up to 28 pieces of data, not all of which were associated with security. The complicated path required for paperwork was prone to errors and delays, with security departments often blamed for a visitor's access being denied at the destination site.

Conflicting site requirements (e.g., ES&H and contractor corporate-wide badges) also hindered the process.

Incompatible badges and access control systems

Each site's badge had a different look, used colors differently, displayed different information, and used differing technologies for automated badge reading. These technologies include the use of magnetic strips (on either edge of the badge), Weigand, Barium Ferrite sensing, bar coding, and proximity sensing. With such significant differences between the badges of the major facilities, there was no practical way to honor all, or even most, of the badges at any of the sites.

The need to be rebadged to visit another site required a stop at the badge office upon arrival, with delays ranging from one-half to many hours. There were costs also associated with the production and tracking of the badge.

Communication of need to know

Some classified visits involve access to information that requires special protection due to its relevance to sensitive areas. Access to this information required an approval from the agency owning it. This access authorization (Sigma) was often given on a visit-by-visit basis. The organization approving and sending the Sigma approval resided in Washington D.C., and the communication path for the Sigma was paper-based and different than for sending the clearance information.

Impacts on the DOE

The problems briefly mentioned above were seen to be the result of a focus on denying access to unauthorized individuals, rather than allowing access to authorized individuals. The need for change was brought about by three factors:

1) There was an increase in security awareness throughout the 80's. This resulted in a substantial upgrade of the physical security infrastructure and led to new security initiatives in the DOE. Many of the new systems and rules increased the complexity of classified visits.

2) The DOE strictly followed its own security rules. Ad hoc exceptions, bypasses, or head turning in areas of physical and personnel security were quite rare throughout the DOE complex. Even the highest managers were bound (and sometimes inconvenienced) by the same rules that applied to the average worker.

3) There was a need to work more effectively. Cost benefit analysis, driven by the pervasive cost cutting in the federal government, identified not only the direct cost of classified travel (badge offices and clearance departments), but also the costs associated with delays to the traveler. These costs were high.

DOE's New Vision for Access Control

Ed McCallum (NN-51, Director of the Office of Safeguards and Security) and his staff developed a new vision of access control. This vision is:

- Access should be controlled through any door in the complex by using a DOE badge.
- New access control systems should be transparent, with increased security benefits.

DOE's goal is to have a compatible, complex-wide automated access control system. The system needs to be based on the critical elements of a classified visit (Figure 2).

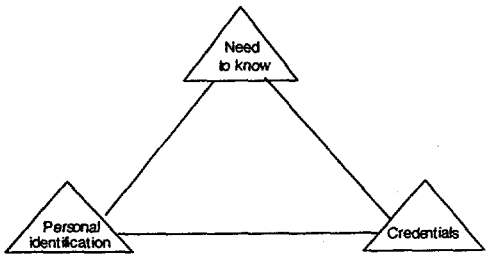


Figure 2. Critical elements of a classified visit.

Credentials

The credential of a traveler is the DOE-granted clearance. The badge issued to the traveler bears evidence of that clearance. Within the DOE, and now with reciprocity throughout the federal government, the clearance indicates that after an appropriate background investigation, the individual is determined trustworthy.

Personal Identification

Security precautions are for naught if the person badged and given access is not the same person whose clearance and need to know have been established. Many techniques are used to establish a person's identity including something that the person:

- knows (PIN or name)
- has (badge or license)
- is (biometric)

Need to Know

In high security programs, a person's identification and trustworthiness is not sufficient for him or her to be given access to information. A clear need for a person to know must be established before access can be granted. In the DOE, this need to know is established by the organization "owning" the information. For example, access to nuclear weapons design information is determined by the Defense Programs. However, the fact must be recognized that it is the person holding or controlling the information who ultimately decides whether or not to provide the information.

The DOE developed a phased approach to implement their vision for access control involving:

- Revised visitor access control procedures
- Standardized badge electronic media
- Badge readability by visitor control offices
- Badge readability by any access control system in the complex
- A fully automated complex-wide visitor/site access control system

The DOE's vision, goal, and approach led to the DOE Complex-Wide Access Control (CWAC) system. The resulting interconnected systems provide the connection between physical security and personnel security systems required to provide a truly high security, transparent, complex-wide access control system.

Its cornerstones are a personnel security network and databases, a set of policies and procedures and hardware for integrating automated access control systems, and the standard DOE security badge. This system is called the DOE Integrated Safeguard and Security (DISS) system. Each cornerstone is discussed in the next section.

DOE Integrated Safeguards and Security System

The modifications of the DOE Integrated Safeguards and Security system (Figure 3) began in June of 1993 with the task of automating the system used to obtain and process security clearances. It followed the DOE Automated Visit Access Control System (DAVACS) which was DOE's first big step in eliminating the paperwork required to verify visitor clearances.

Substantial savings in resources and time were anticipated by the adoption of an automated system to enter, transmit, process, and track the information and status associated with the requesting and granting of a DOE security clearance. This project was expanded a year later, replacing DOE's Central Personnel Clearance Index (CPCI) with a new Personal Security Database (PSDB) and automating the Weapons Data Access Control System (WDACS) used to track and communicate need-to-know decisions made by DOE's Defense Programs. A link to the Safeguards and Security Information Management System (SSIMS) was also added to provide information needed in the clearance granting process.

Automated Access Control Integration

In order to provide true nation-wide access control, the DOE needed to define the information needed to make access control decisions, provide the communication interface and protocol necessary to store and retrieve this information in a central database, and determine the rules that govern the operation and use of this data. Integrated automated access control systems require a means to enroll badge, PIN, weight, and biometrics information about individuals; a central database to store this information along with the individual's current clearance status; and access control systems that use this information to make access control determinations. The major elements of integrated automated access control systems were demonstrated this spring, and the initial field-test site at the Oakland Operation Office is scheduled for activation in late August.

The scenario for automated access control integration is shown in Figure 4.

1. The individual is badged and enrolled in his or her local site access control system (ACS). The local badge office takes responsibility for verifying the identity of the individual.

2. Enrollment data, including badge, PIN, weight, and biometric information is transmitted to a central Visitor Access Data Base, where it is stored in association with the individual's clearance data.

3. The individual travels to another site and attempts to enter a security area protected by an automated access control system.

4. The ACS reads the person's badge and determines that the person is not enrolled locally.

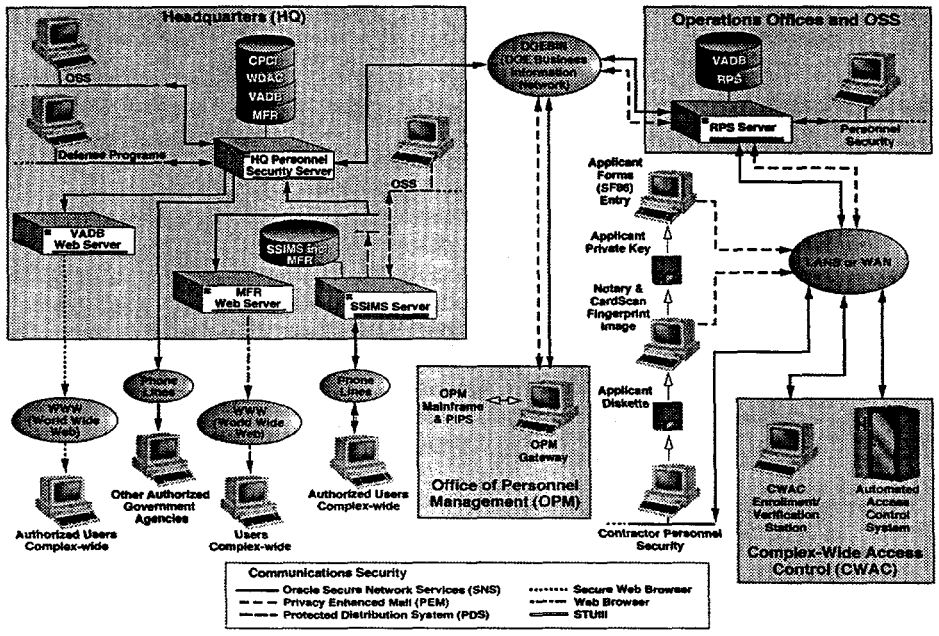


Figure 3. DOE Integrated Safeguards and Security (DISS)

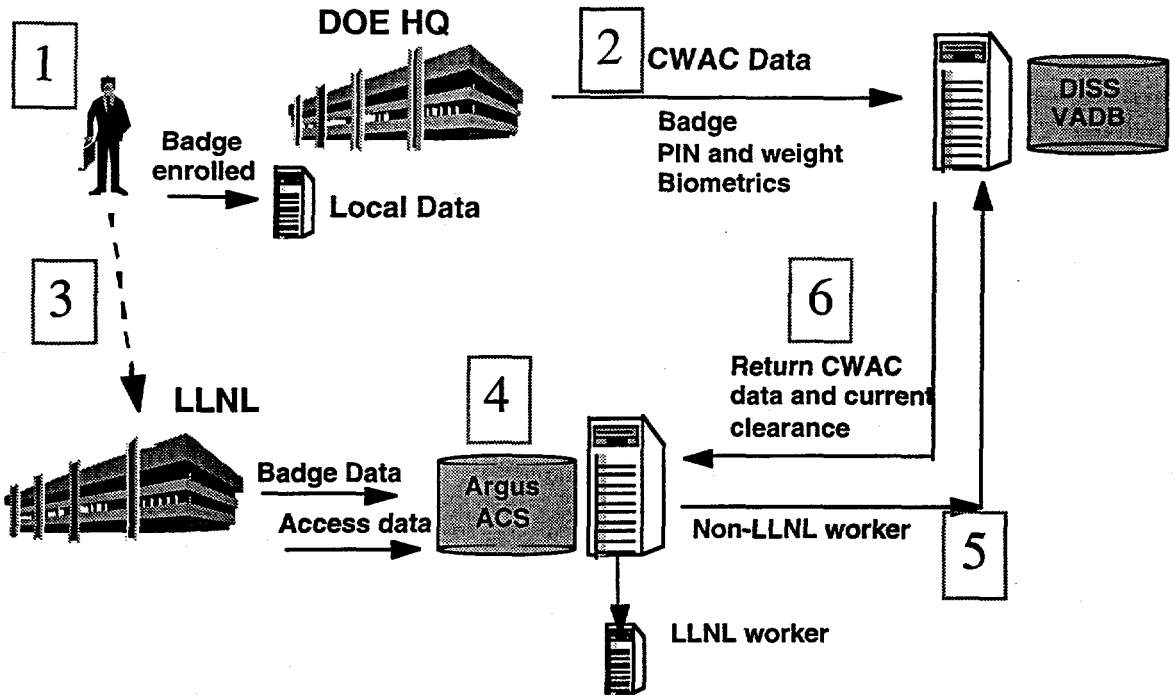


Figure 4. Integrated Automated Access Control Diagram

5. The ACS requests access control information from VADB.

6. VADB returns the access control information, along with the current clearance, to allow the ACS to make an access control decision. If the visitor's PIN is verified, his or her badge and clearance are validated, and weight measurement confirms the individual is alone, the person is allowed to proceed (assuming any other site specific requirements have been satisfied).

DOE Standard Badge

The DOE standard badge is being issued to all federal and non-federal employees as an accountable credential indicating clearance level and association with the DOE. The DOE badge is based on a standard visual appearance and access control technology. The program's goal is to issue only one permanent DOE standard badge per individual. If the individual possesses an access authorization, then the badge issued will exhibit the highest active access authorization, regardless of current work or contract activities.

Badge Front

The front of the badge displays a photo image of the badge owner along with an indication of the individual's clearance level. It also contains a unique badge serial number, identifies the issuing DOE Operations Office and facility, and indicates whether the person is a federal or DOE-contractor employee. A holographic overlay is applied to help deter attempts at forgery.

Back of Badge

A magnetic strip on the back of the badge is encoded with the unique badge serial number, the individual's social security number (SSN), and a random encryption key. The encryption key, recorded on the magnetic strip, is used to encrypt PIN and weight information before they are stored in a local access control database or the Visitor Access Control Database. This same key is read from the badge at each visitor attempt to pass through an access control point. It is used to decrypt the PIN and weight information retrieved from storage and compare it with PIN and weight information provided by the visitor. As an important part of the complex-wide information protection strategy, the encryption key is not recorded anywhere in the system other than on the badge.

Common Badging and Access Control

The Department of Energy took a systems approach when formulating and implementing the projects and policies leading to CWAC. Although it was necessary for the entire complex to use a compatible badge, this was not sufficient to meet the goal of door-to-door

access. The information on the badge and in central databases and the way that information was used to grant access at remote sites were key to the secure operation of the system. As CWAC is fielded at more sites in the coming year, we will be able to measure the reduced manpower and delays and will benefit from improved security for classified visits between sites.

We are beginning to observe a systems approach for a common federal badge, with exchanges of information between the largest badge-using agencies. We believe that the same successful process that led to the creation of the DOE Integrated Safeguards and Security system can be used effectively for the federal government.

Once that is done, DOE's tools and systems will be ready to provide lessons learned and perhaps even direct usable pieces for the new Federal Access Control System.

References

DOE Integrated Safeguards and Security - Personnel Security Database System Requirements Specification, Everett Wheelock, Lawrence Livermore National Laboratory, November 1995

Personnel Security Network and Databases Concept of Operations, Version 4, Lawrence Livermore National Laboratory, October 1995

Functional Requirements Document for the DOE Standard Badge, DOE Office of Safeguards and Security, February 1, 1996

Complex Wide Access Control Functions and Requirements Document, Version 1.1, Dan Johnson, Lawrence Livermore National Laboratory, January 18, 1996

Argus Functional Description, UCRL-TB-118718, October 1994, Lawrence Livermore National Laboratory

DAVACS functional description DAVACS DOE Automated Visitor Access Control System, UCRL-MI-113646, Lawrence Livermore National Laboratory, July 1993

Visitor Access Data Base Interface Control Document, Version 1.0.2, Everett Wheelock, Lawrence Livermore National Laboratory, January 16, 1996

Disclaimer

UCRL-JC-124698

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