PNL--8180

DE92 017747

REVIEW OF THE U.S. DEPARTMENT OF ENERGY
CLASSIFIED VISITS PROGRAM

S. W. Martin
M. H. Killinger
M. A. Segura

July 1992

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest Laboratory
Richland, Washington 99352

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

EXECUTIVE SUMMARY

This review examines the U.S. Department of Energy (DOE) Classified Visits Program, which is administered by the Office of Safeguards and Security. The overall purpose of this analysis is to 1) ensure that DOE policy and implementing procedures are appropriate to maintain U.S. national security intentions, 2) evaluate the effectiveness of the process used across the DOE complex, and 3) recommend changes which will enhance the overall efficiency of the process while maintaining the program's integrity.

The study reviewed statutory and Presidential directives that set forth the philosophy of protecting classified U.S. information; these national-level policies have guided the development of the DOE policy and procedures regarding classified visits. The review identified the following basic tenets which must be ensured by the DOE Classified Visits Program: 1) only individuals who possess a current and valid security clearance are granted access to classified matter, 2) individuals must have a need-to-know (the matter) in the performance of their duties, and 3) visitors are positively identified at the visited site prior to being granted access to classified matter.

Review of the DOE implementing order (DOE 5631.4, Control of Classified Visits) and subsequent onsite review of program implementation at several sites revealed that the DOE program fulfills the basic tenets of U.S. policy. However, the DOE implementing order levies additional requirements that tend to reduce efficiency and may serve to degrade the integrity of the program by placing certain responsibilities at management levels above what is necessary. The study determined that the required Division Director-level signature, as specified in the DOE Order, is unnecessary. The study also revealed that system operators' inability to get the "proper" signature on DOE F 5631.20 form, "Request for Visit or Access Approval," delays processing requests, while improper signatures have resulted in "findings" during past inspections. Although a signature at the visited site may be desirable, the level of required signature could be lowered considerably without sacrificing the

integrity or effectiveness of the process.

The DOE's Classified Visits Control System (CVCS) has the potential to be an innovative and capable system used to verify and pass individual clearances. However, the study shows that the CVCS's overall effectiveness is not being fully realized across the DOE complex. This is because 1) most personnel are not yet adequately trained on how to use the system, although progress is being made, and 2) some major DOE and DOE contractor sites are not yet linked to CVCS.

Based on analysis of on-site review results, combined with a comparison of the current Classified Visits Program with required U.S. policy, this study makes the following recommendations:

- Eliminate the requirement for management signatures for "need-to-know" and "operational approval," which do little or nothing to enhance the integrity of the program, while at the same time degrade efficiency.
- Delegate authority for clearance verification and certification to those personnel within local visit control offices.
- Extend CVCS to all major DOE and DOE contractor sites, and make its consistent utilization mandatory.
- Headquarters can ensure program standardization by providing effective training to all CVCS system users. Training will also ensure the full potential of the tool is achieved.
- Attempt to integrate CVCS and the process used to pass weapons data and uranium enrichment programmatic access approval.
- Make software modifications to CVCS to capture the full potential of the system's integrated databases.

CONTENTS

EXECUTIVE SUMMARY	iii
1.0 INTRODUCTION	1.1
2.0 SYSTEM ELEMENTS REQUIRED BY U.S. POLICY	2.1
2.1 ASSUMPTIONS	2.1
2.2 SYSTEM INTEGRITY	2.1
3.0 COMPARISON OF ESSENTIAL ELEMENTS VERSUS CURRENT DOE SYSTEM	3.1
3.1 THE THREE BASIC TENETS	3.1
3.1.1 Verification and Certification of Security Clearance	3.1
3.1.2 Verification of Need-To-Know	3.2
3.1.3 Positive Identification of Visitors	3.3
3.2 IDENTIFIED PROBLEM AREAS THAT DEGRADE EFFICIENCY	3.3
3.3 INCONSISTENCIES IN PROGRAM IMPLEMENTATION	3.5
3.4 USER COMPLAINTS ABOUT CVCS SYSTEM	3.5
3.5 MULTIPLE SYSTEMS	3.6
4.0 RECOMMENDATIONS	4.1
4.1 POLICY AND PROCEDURAL REQUIREMENTS	4.1
4.1.1 Need-To-Know Certification at Traveler's Site	4.1
4.1.2 Verification and Certification of Current and Valid Clearance	4.1
4.1.3 Need-To-Know Certification at Visited Site	4.2
4.2 USE OF ONE SYSTEM WITHIN DOE	4.2
4.2.1 Contractor Use of CVCS	4.2
4.2.2 Training in CVCS	4.3
4.2.3 Integration of CVCS with Other DOE Program Approval Requirements	4.3
4.3 ARCHITECTURAL MODIFICATIONS TO CVCS SYSTEM	4.3
4.3.1 More Auto-fill Fields through Integrated DISS System	4.4
4.3.2 Modification to Accommodate Changes within Data Fields	4.4
4.3.3 Notification of Pending Visits	4.4

4.4	RECOMMENDED PROCESS FOR HANDLING CLASSIFIED VISITS	4.4
4.5	ADDITIONAL RECOMMENDED ANALYSIS	4.4
APPENDIX A	- REVIEW OF APPLICABLE U.S. NATIONAL SECURITY POLICY DOCUMENTS	A.1
APPENDIX B	- REVIEW OF DOE ORDER 5631.4, CONTROL OF CLASSIFIED VISITS	B.1
APPENDIX C	- RESULTS OF ONSITE REVIEWS	C.1
APPENDIX D	- RECOMMENDED PROCESS FOR DOE CLASSIFIED VISITS PROGRAM	D.1
APPENDIX E	- REVIEW OF DEPARTMENT OF DEFENSE POLICY REGARDING CLASSIFIED VISITS	E.1

1.0 INTRODUCTION

This study identifies those actions essential to ensure that visitors to DOE facilities obtain access to classified matter only if they have the appropriate clearance and have a verified need-to-know. The analysis determines whether DOE is meeting or exceeding those requirements and makes recommendations to improve the system's efficiency while maintaining its integrity.

The following approach was used in making the study. First, U.S. national security policy related to the protection of classified matter and what that policy strives to achieve was identified and reviewed. Second, from those policy requirements, a basic set of tenets which must be met and ensured by the DOE Classified Visits Program, was determined. Based on those tenets, a system that meets the letter and spirit of applicable U.S. policy was defined. Third, by reviewing the current DOE implementing policy and procedures, deficiencies or excesses in the DOE system as compared to a system that meets the basic tenets, were determined. Onsite reviews were conducted at several DOE and DOE Contractor sites to determine how the Classified Visits Program was actually being implemented across the DOE complex.

The text of this document is oriented toward the results of the study. Information gathered and used for analysis has been documented in the attached appendices. Appendix A contains an in-depth review of applicable U.S. national security policy. DOE Order 5631.4, Control of Classified Visits, is reviewed in Appendix B. The results of the onsite reviews and a graphical depiction of the current process are contained in Appendix C. A recommended process for the DOE Classified Visits Program is described in Appendix D, and Department of Defense policy regarding classified visits is reviewed in Appendix E. Recommendations are provided in Appendix D; the other appendices contain the results of background research.

2.0 SYSTEM ELEMENTS REQUIRED BY U.S. POLICY

This chapter sets forth three conditions needed to maintain the integrity of the DOE Classified Visits Program. Applicable U.S. national security policy documents are reviewed in Appendix A.

2.1 ASSUMPTIONS

For the purposes of this assessment, the following assumptions have been made.

- Material exists that requires protection for the purpose of maintaining the national security. This includes all levels and categories of classified matter.
- There is in place a mechanism which allows DOE to determine the trustworthiness of an individual and to thereby certify that individual to have access to classified matter by granting that individual a security clearance.

2.2 SYSTEM INTEGRITY

To maintain the integrity of the DOE Classified Visits Program, there exist three distinct and separate determinations which must be made on a case-by-case basis. All three conditions or tenets, which are based on statutory and Presidential directives, must be met or the integrity of the entire system becomes questionable.

1. Current/valid clearance: The individual possesses a valid clearance at the level required for the access requested.
2. Need-to-know: The individual has a verified need-to-know the matter in the performance of their duties.

3. Positive Identification: Visitors being granted access are indeed who they purport themselves to be.

These three tenets are used throughout the analysis to identify those policy and procedural steps in the existing system that contribute to maintaining system integrity as opposed to those which do not.

3.0 COMPARISON OF ESSENTIAL ELEMENTS VERSUS CURRENT DOE SYSTEM

While DOE Orders and existing procedures are consistent with the philosophy of U.S. national security policy, the Classified Visits Program lacks efficiency and may inadvertently degrade the system's effectiveness because of certain excessive requirements intended to provide added protection.

This chapter examines current requirements and the manner in which DOE fulfills them. Pertinent extractions from DOE Order 5631.4, Control of Classified Visits, have been documented in Appendix B. Analytical results are based on review of documentation, onsite reviews of program implementation, and interviews of DOE security professionals responsible for oversight and implementation of the DOE Classified Visits Program. Results of program reviews are fully documented in Appendix C, which also contains a diagram of the current DOE classified visits process.

3.1 THE THREE BASIC TENETS

The following is an analysis of DOE compliance with the three basic tenets listed in Section 2.2.

3.1.1 Verification and Certification of Security Clearance

In order to ensure that only authorized visitors access classified matter, DOE requires that security professionals verify and certify by signature that a traveler does indeed possess a valid security clearance. This requirement is currently being met in practice. Verification is performed by those who have access to the information necessary to make this determination (usually facilitated by a computer database). While most DOE field offices delegate clearance certification authority to contractors (who have their own clearance information), two sites reviewed had not. Routing the form from the contractor's visit control office to the DOE field office for certification signature degrades the efficiency of the process without adding effectiveness.

3.1.2 Verification of Need-to-Know

DOE has elected to add management-level approvals above that necessary to adequately establish whether or not a traveler has a justified need-to-know.

Review results indicate that the process has become so routine that those having "need-to-know" and "operational approval"^(a) signature authority sign nearly all requests which are presented to them. Most often these signatures are based on the assumption that others within the process have fulfilled their responsibilities regarding the appropriateness of the classified visit.

During the site reviews, no one could provide convincing justification for the Division Director-level management signature certifying need-to-know on the outgoing (visitor's) side of the process. The signature is obtained only because it is required. Most security professionals felt that a need-to-know determination is the primary responsibility of the individual making the disclosure. In fact, this is valid for anyone disclosing classified matter, regardless of whether or not the recipient is in a travel status. Cleared employees who are not in a travel status gain access to classified matter from others without 1) passing their clearance, or 2) their management certifying by signature the employee's need-to-know. Need-to-know is typically worked out between the parties directly involved.

On the incoming (host's) side, determination of need-to-know (i.e., operational approval) becomes an extremely important element of the process. The individual best able to make this determination is the host, which is usually the same individual who will be disclosing classified matter to the visitor.

(a) "Operational approval" is the term for need-to-know certification at the visited site.

Again, interviews of DOE personnel involved in the process agreed that obtaining a certification signature for operational approval has usually become a matter of routine, something required by DOE Order 5631.4. Those individuals with operational approval signature authority are signing nearly all requests, usually with little or no awareness of how the visitor justified their need-to-know. Seldom does the certifying official contact the host directly.

Instead, visit control personnel at most sites reviewed are contacting the host and determining 1) whether the visitor is expected, and 2) verification of access requirements. This simple process may be sufficient to verify need-to-know via contact from security personnel to the host, who is ultimately responsible for the disclosure of classified matter to the visitor.

3.1.3 Positive Identification of Visitors

The primary method of establishing the identity of a visitor who will be accessing classified matter is via a picture identification. The majority of those interviewed felt that this is efficient and reliable. Because this action is completed by disinterested security personnel, this tenet is met both effectively and efficiently.

It should be noted that there are enhanced forms of technology for establishing positive identification, such as "smart badges" which employ biometrics (fingerprint, hand geometry, eye mapping). There are ongoing, independent studies within DOE examining the use of such technologies.

3.2 IDENTIFIED PROBLEM AREAS THAT DEGRADE EFFICIENCY

The following problems were identified directly from interviews or from analysis of information obtained during reviews.

Requirement for Division Director-level Management Signatures. The existing DOE Order 5631.4 requires Division Director-level management signatures for certifying need-to-know. This requirement causes delays in

processing requests because the forms have to be routed out of visit control channels for signature and then back again. Additional delays are caused when the responsible individual is not available for signature.

Visitors Submit 5631.20 Form Late. Visitors often do not submit their 5631.20 form within the time frame prescribed, usually ten days in advance. While it is understood the system must accommodate the unexpected short-notice trip, far too many forms are submitted a day or two prior to travel for no justifiable reason.

Lack of Access to CVCS. Not all major DOE and DOE contractor sites are linked to CVCS, which creates several problems. The requests must be processed in a different manner, primarily by facsimile. In those instances where major DOE contractors do not have CVCS or authority for their own classified visits program, the processing time is increased because the requests must be routed back and forth between the contractor and the DOE Field Office having oversight.

Redundant Local Databases. With the exception of DOE-Headquarters, virtually all DOE and DOE contractor sites reviewed are maintaining independent (and redundant) local databases. Visit requests that are processed via CVCS are again entered into another separate, local database.

When the sites were queried about the need for an independent classified visits database when they had access to CVCS, virtually all responded that CVCS is not a complete repository. They believe that only requests transmitted via CVCS can be retained in the CVCS database, and that it is not possible to make records entries into CVCS of other agency visits or those DOE visits to or from sites that are not linked to CVCS. Therefore, the sites reason, since CVCS does not contain a complete record of the visit program for a site, a separate database with all visits is necessary.

This demonstrated a deficiency in training and user understanding of CVCS. The CVCS is, in fact, capable of record-keeping, even for visits not transmitted via the system.

No Discrimination Between Pending Requests. "Pending" CVCS listings do not discriminate old pending requests from those requests entered since the last listing. Therefore, a manual comparison is required to segregate those pending requests which are being processed--but not yet approved--from those new requests which require action.

3.3 INCONSISTENCIES IN PROGRAM IMPLEMENTATION

Reviews of various sites indicate the following inconsistencies in program implementation.

Signatures Required on the DOE F 5631.20 Form. Most sites require some form of management-level certification of need-to-know as a step of processing outgoing requests. However, the level of signature required is never the same. All had delegated the responsibility to management levels below that of Division Director. Some contractors were having difficulty finding a management level which equated to that of the DOE Division Director.

Operational approval signatures for visits on the incoming side of the process is entirely different. Some sites are obtaining the signature while others are not. Where signatures are being obtained, especially those locations where program responsibility is retained by DOE and not delegated to contractors, numerous interactions are involved. We do not consider many of these interactions to be cost-effective or worth the time they require. At some locations the process for obtaining operational approval signatures is ignored; the information is obtained telephonically by visit control from the host.

Delegated Authority to Contractors. Most DOE field offices have delegated visit control authority and responsibility to the major DOE contractors under their administrative jurisdiction, while a few have not.

3.4 USER COMPLAINTS ABOUT CVCS SYSTEM

Lack of Access. Not all major DOE and DOE Contractor sites are

connected to CVCS. This creates the need to use more than one method of transmitting requests, even within DOE.

Untapped Capabilities. CVCS is not as user-friendly or as "smart" as it could be. For example, numerous complaints were made about why certain fields of data do not auto-fill, similar to the way a traveler's clearance number does. Beyond the clearance number, there are only two additional entries required for verification and then certification of a traveler's clearance: the clearance level and the date the clearance was granted. With better integration between the Central Personnel Clearance Index (CPCI) and CVCS systems, all three fields should fill automatically when the traveler's personal information (name, Social Security number, date of birth) is entered. Correction of this problem could be effected through software architecture and is well within the capability of the DOE Integrated Security System (DISS).

Difficult to Make Changes. CVCS is not very accepting of errors. CVCS includes several fields of information that cannot be changed after entry. While there are some fields that should remain unchangeable, there are possibly some that a system user should be able to change when an error is made. Almost all users complained that they dislike having to "cancel" a visit request and create a complete new visit request record because of an error in one of the unchangeable fields.

Lack of Training. A perception of receiving inadequate training was an issue at all sites reviewed. Some sites reviewed claimed to have never been trained on CVCS. An excellent example of lack of knowledge is that, with the exception of Headquarters, no site reviewed was aware that CVCS could be used as a record repository for visit requests that were passed to sites not linked to CVCS.

3.5 MULTIPLE SYSTEMS

Within DOE, there is one primary system (i.e., CVCS) for verification, certification, and transmission of security clearances from one location to another. However, there exist two additional independent systems for

"passing" special program access approval. The largest independent system is the Weapons Data Access Control System (WDACS) operated by DP-23. WDACS is a Headquarters database that is linked to all 14 sites comprising the weapons complex. Clearances are still verified and certified by security personnel; however, the visit requests are then forwarded to DP-23 for approval. In essence, DP-23 is acting as a visited site and providing a type of "operational approval" which is then retransmitted to the actual visited site via WDACS.

Access to uranium enrichment programs and sites requires approval by NE-30. Requests are sent to NE-30 by facsimile. NE-30 then retransmits the approved request, again via facsimile, to the involved site.

This additional processing--through a separate system--degrades the efficiency of the process. While program office approval for weapons data and uranium enrichment is expected to continue, a more efficient process which integrates program office approval into CVCS would be a beneficial to DOE.

4.0 RECOMMENDATIONS

Recommendations have been listed in priority of their importance. Additionally, those which are achievable through use of existing resources receive the greatest attention.

4.1 POLICY AND PROCEDURAL REQUIREMENTS

DOE Order 5631.4, "Control of Classified Visits," is currently under revision. Those policy and procedural recommendations listed below, which are deemed valid, should be incorporated. Due to the long-ranging effects of such changes, we recommend a "task force" approach to selecting policy and procedural changes. Such an approach will ultimately enhance overall acceptance of program changes. The task force recommended would be composed of DOE (and possibly DOE Contractor) security professionals who provide oversight of the Classified Visits Program. Subsequent to determination and agreement of the policy changes, procedural and implementation changes will be required.

4.1.1 Need-to-know Certification at Traveler's Site

Eliminate the requirement for a management-level certification signature on the outgoing side of the process. Consider eliminating the signature requirement entirely. The majority of security professionals and management personnel interviewed agree that need-to-know determinations remain an individual responsibility and rest with the individual who will be disclosing the information.

If DOE desires responsibility or accountability signatures concerning need-to-know on the outgoing side of the process, it should lie with the traveler or be placed at the lowest possible management level.

4.1.2 Verification and Certification of Current and Valid Clearance

Place responsibility for clearance verification and certification with

the visit control office at the traveler's place of employment (DOE or DOE Contractor). Their office has the tools (CPCI, CVCS or local systems) to perform the function and is a responsible, disinterested third party to the process. At those locations where DOE has not delegated responsibility to contractors under their jurisdiction, unnecessary processing of the form is required to obtain a certification signature. In these instances, the DOE person signing the form usually does not verify the clearance at all, but signs the form assuming the contractor's visit control office has done so.

4.1.3 Need-to-know Certification at Visited Site

Eliminate the requirement for an "operational approval" signature. The tenet of verification of need-to-know is best satisfied between the visitor and the host. Currently, Visit Control personnel contact the host; this can be accomplished without the need for a signature and should be sufficient to satisfy the intentions of national security policy.

If DOE desires to have a written record of certification, then the host's signature can be required. This has legal advantages, but would add processing time.

4.2 USE OF ONE SYSTEM WITHIN DOE

Use one system, CVCS, within DOE because consistency and uniformity can contribute significantly to the effectiveness of the nationwide DOE Classified Visits Program. The more uniform the process from site to site, the more likely the system will facilitate work and travel rather than degrade performance.

4.2.1 Contractor Use of CVCS

Extend CVCS to all major DOE and DOE contractor sites. CVCS is a well thought out process and a capable tool, specifically designed to facilitate transmitting classified visit requests from one location to another. Of those sites reviewed, we recommend extension to two specific DOE contractors,

Pacific Northwest Laboratory, approximately 2,000 visits annually, and Westinghouse Hanford Company, approximately 1,200 visits annually. Use of CVCS should be mandatory. While CVCS has been extended to Los Alamos National Laboratory and Rocky Flats, they are not using CVCS.

4.2.2 Training in CVCS

Train all users of CVCS. DOE-Headquarters conducted four separate, two-day CVCS training sessions in 1991, during which a total of 30 personnel from most major field offices attended. However, CVCS users repeatedly expressed a desire for training on use of the system. This training would be best received if provided by those relatively few knowledgeable users of CVCS, rather than technical system managers or engineers. Such training would also ensure the uniformity that will enhance overall system effectiveness.

4.2.3 Integration of CVCS with Other DOE Program Approval Requirements

Attempt to integrate classified visit requests with additional program approvals, specifically those involving Weapons Data and Uranium Enrichment programs (DP-23 and NE-30, respectively). The requests could all be processed electronically via CVCS. This would not only reduce facsimile traffic between program offices and sites, but would eliminate a completely separate system for transferring clearances and program access approvals for weapons data (i.e., WDACS).

CVCS architecture could possibly be modified to accommodate a program office approval as part of the process. Instead of the visited site, the program office could change the request from pending to approved. Interactive CVCS terminals would be required at both DP-23 and NE-30. The feasibility of this recommendation will require additional research.

4.3 ARCHITECTURAL MODIFICATIONS TO CVCS SYSTEM

The following architectural modifications to the CVCS system are recommended.

4.3.1 More Auto-fill Fields through Integrated DISS System

The system architecture should auto-fill as many fields as possible. DISS was created to reduce workload and it should be used to its full capacity.

4.3.2 Modification to Accommodate Changes Within Data Fields

Evaluate CVCS to determine exactly which fields should not accommodate changes. If there are fields that cannot be currently changed that could be modified to accept changes, without degrading the system's integrity, they should be modified.

4.3.3 Notification of Pending Visits

Enable CVCS to produce useful lists of pending visits. Possible types of listings are 1) visits entered into CVCS since the last printing; 2) visits by first day of visit, chronologically, to identify those visits occurring first and therefore require processing first; 3) a system that prints a visit request automatically at the visited site when it is initially transmitted via CVCS; and 4) a query capability to simply view visit requests entered since the last "pending" printout.

4.4 RECOMMENDED PROCESS FOR HANDLING CLASSIFIED VISITS

We developed a process for handling classified visits that we believe is effective and efficient. A narrative and flow chart of the process appears in Appendix D.

4.5 ADDITIONAL RECOMMENDED ANALYSIS

1. Consider doing a concept study concerning the need to pass clearances at all between DOE sites which have access to DISS. The concept of passing a clearance between sites is to provide verification of an individual's clearance to a location that does not have the ability to verify the

traveler's clearance themselves. With the integration and implementation of DISS, of which CVCS is part, virtually every site that is linked can verify a traveler's clearance themselves.

2. Review related studies of the National Industrial Security Program for possible impacts on the Classified Visits Program.

APPENDIX A

REVIEW OF APPLICABLE U.S. NATIONAL SECURITY POLICY DOCUMENTS

APPENDIX A

REVIEW OF APPLICABLE U.S. NATIONAL SECURITY POLICY DOCUMENTS

This appendix is divided into two parts, one pertaining to Restricted Data (RD) and the other to National Security Information (NSI) and personnel security.

Restricted Data

The U.S. Department of Energy's (DOE's) authority to establish and maintain a security program to regulate access to restricted data and special nuclear material is derived from both statutory law and Executive Order. The Atomic Energy Act of 1954 (AEA) is the statutory authority.^(b) Sections 141-145 establish a general mandate to control the dissemination of restricted data. Section 161 gives DOE the authority to promulgate rules and regulations necessary to perform its functions.

Section 161 General Provisions: Provides that the Atomic Energy Commission (and its successor, DOE) may establish by rule, regulation or order, necessary standards and instructions to govern the possession and use of special nuclear material, source material, and by-product material, and states that the Commission is authorized to establish regulations and orders necessary to protect Restricted Data and to guard against the loss or diversion of special nuclear material. The Commission may also "make, promulgate, issue, rescind, and amend such rules and regulations as may be necessary to carry out the purposes of [the] Act." This section sets forth the authority necessary to perform

---

(b) DOE was established in 1977 by the Department of Energy Organization Act, and acquired certain responsibilities which had been vested by law in the Energy Research and Development Administration (ERDA) by the Energy Reorganization Act of 1974. These functions, originally assigned to the Atomic Energy Commission (AEC) by the Atomic Energy Act of 1954, had been inherited by ERDA upon the abolition of the AEC in 1974.

the functions of DOE.

Section 141, Policy: Establishes a general mandate to control the dissemination of Restricted Data "in such a manner as to assure the common defense and security."

Section 143, Department of Defense Participation: Provides that employees of the Department of Defense (DOD), DOD contractors, and members of the armed forces may be authorized access to Restricted Data required in the performance of their duties provided that DOD personnel security procedures and standards ensure that such access will not endanger the common defense and security. Established personnel and security procedures of the agency must be adequate and conform to the standards established in Section 145, "Restrictions," to ensure the character, associations and loyalty of the individuals who are granted access.

Taken together, these sections of the AEA provide statutory authority for establishing and implementing a DOE security program for controlling access to Restricted Data and special nuclear material.

National Security Information and Personnel Security Issues

The below listed Executive Orders provide authority for DOE to establish and maintain an effective personnel security program to ensure the loyalty and trustworthiness of federal employees and to control access to classified matter. They are identified only to establish the basis upon which DOE grants individuals access to classified matter, which is more a part of the clearance granting process than the passing of one's clearance.

Executive Order 12356, "National Security Information," April 2, 1982: Provides requirements concerning classification of information, and establishes controls on access to National Security Information.

Executive Order 10450, "Security Requirements for Government Employees,"
April 29, 1953, as amended: Establishes the requirement for determining that all federal employees are loyal, reliable, trustworthy and of good conduct and character. Each agency will establish and maintain an effective personnel security program.

Executive Order 10865, "Safeguarding Classified Information Within
Industry," February 20, 1960, as amended: Establishes the basis for the industrial security program for civilian personnel.

APPENDIX B

REVIEW OF DOE ORDER 5631.4, CONTROL OF CLASSIFIED VISITS

APPENDIX B

REVIEW OF DOE ORDER 5631.4, CONTROL OF CLASSIFIED VISITS

This section highlights those areas of the order which directly affect program integrity. The three basic tenets which must be met prior to disclosing classified matter are either clearly stated or implied in the "Policy" section of the directive. They are:

- Only authorized persons [those possessing a current and valid security clearance] receive access to classified matter.
- Need-to-know [as determined by a division director or higher official] will be a basic principle to be observed.
- Positive identification is implied in the determination of "authorized persons."

Paragraph 6 "Definitions" contains several pertinent entries which currently guide DOE policy and procedures.

6a. Access Authorization or Security Clearance: "...determination that an individual...is eligible for access to restricted data, other classified information, or special nuclear material.'

6f. Classified Visit: "...any visit in which an individual is granted access to classified information or in which he/she visits a classified facility...after an official determination has been made by a division director or higher official that he/she needs this access in the performance of his/her official duties."

6p. Need-To-Know: "...an official determination, by a division director or higher official, that a...properly cleared individual requires access to the specific classified information in the performance of official duties."

6q. Operational Approval: "...a determination by the Head of a field organization or the Head of a Headquarters organization that a proposed visit to a facility under his/her jurisdiction is feasible, is subject to limitations, and that the visitor has a 'need-to-know'."

Paragraph 7, "Responsibilities and Authorities," sets forth pertinent requirements which DOE is using to assure the integrity of the classified visit program:

7b(1) Director of Safeguards and Security (SA-10):

- Certifies on DOE F 5631.20, "Request for Visit or Access Approval" (formerly DOE Form DP-277), the following:
  - DOE Clearance Type
  - DOE Clearance Number
  - DOE Clearance Date

7b(3) Director of Military Application (DP-20): provides programmatic approval for requests for visits which deal with access to Weapons Data (Ref: DOE 5610.2, Control of Weapon Data).

DP-23 maintains a separate computer system, Weapons Data Access Control System (WDACS) within the weapons complex through which they pass 17,000 security clearances and programmatic access approvals annually.

7c(2) Uranium Enrichment: NE-30. Processes 300-500 visit requests per year involving the following locations or programs:
Oak Ridge, Portsmouth, Paducah.
Oak Ridge K-25 Plant AVLIS program.
Lawrence Livermore National Lab AVLIS Program.

7d. Secretarial Officers, DOE Staff Officers, and Directors of Headquarters Offices and Divisions shall:

(1 & 2). Grant operational approval and serve as approval authority for requests for classified visits to their respective divisions and organizations [need-to-know certification]. The directive states this authority may not be delegated below the division director level.

7e. Heads of Field Organizations shall:

(1) Implement visitor control system to assure:

- Identity and clearance status of visitor [Positive identification and current/valid clearance certification].
- Limitations with respect to access are established [Need-to-know determination].

(2) Serves as approval authority for requests for classified visits to facilities under their administrative jurisdiction [operational approval]. This paragraph includes an exemption for visits between Weapons Complex sites and the exchange of weapons data between Weapons Complex facilities. Such visits and exchanges are allowed without obtaining the additional programmatic approval.

Paragraph 8. Procedures. The following procedures ensure the integrity of the system is maintained.

8a. Control of Visits to Classified Areas and Facilities: Procedures should ensure:

- Identity and security clearance of the visitor.
- Limitations on access to classified matter or facilities.
- Operational approval of visits is granted or obtained.
- Maintenance of records of all classified visits.

APPENDIX C

RESULTS OF ONSITE REVIEWS

APPENDIX C

RESULTS OF ONSITE REVIEWS

The following information was obtained from personal interviews of individuals involved in management and implementation of the DOE Classified Visits Program. Personal interviews and onsite reviews of program implementation were accomplished at the following locations:

DOE Headquarters

DOE Albuquerque Field Office, Albuquerque, New Mexico

Sandia National Laboratory, Albuquerque, New Mexico

DOE Los Alamos Area Office, Los Alamos, New Mexico

Los Alamos National Laboratory, Los Alamos, New Mexico

DOE Richland Field Office, Richland, Washington

Pacific Northwest Laboratory, Richland, Washington

Westinghouse Hanford Company, Richland, Washington

Each location reviewed divided the Classified Visits Program into two separate functional areas, incoming and outgoing requests. This appendix addresses similarities and differences along those functional lines. A graphical depiction of the current classified visits process appears at the end of this appendix.

C.1 OUTGOING VISIT REQUESTS

All sites reviewed used form DOE F 5631.20 (Request For Visit or Access Approval) to request classified visits. The initial information is normally typed onto the form by clerical staff within the traveler's work area. From this point on, the processing of the form is dependent on several factors:

- whether or not the traveler is a federal employee or a contractor.

- if a contractor, whether or not DOE has delegated to the traveler's place of employment the authority to certify the traveler's clearance.
- if a contractor, whether or not the DOE field office providing administrative oversight has delegated responsibility and authority for the Classified Visits Program.
- if a contractor, whether or not Classified Visits Control System (CVCS) has been extended to the traveler's place of employment.

C.1.1 DOE Federal Employees

The classified visits process is most efficient for federal employees because, in this case, all required approval signatures are within DOE. Once the form has been processed within the traveler's work area, it is routed to the DOE visit control office (either at DOE-Headquarters or the traveler's field office), which in all reviewed areas was a function of the DOE Personnel Security Branch. The form is reviewed for completeness and the traveler's clearance is verified. With the exception of one location, security clearance verification was performed via a locally designed and maintained database rather than via the DOE DISS system. There are two primary reasons for utilization of local independent computer systems to verify a clearance:

- There is a pervasive feeling among field office security professionals that a locally maintained computer database is more reliable and current than the DISS system.
- While the CVCS system automatically provides an individual's clearance number, it fails to provide the level of clearance and the date the clearance was granted. The latter two pieces of data are required in the visit request.

For DOE federal employees, the clearance certification signature is provided by personnel within the DOE visit control office. Once the form is deemed acceptable and the clearance is certified, the form is routed out of

the visit control office for the appropriate need-to-know certification signature, which is typically the traveler's management.

C.1.2 DOE Contractor Employees Where CVCS Has Been Extended

In these instances the processing is not much different than that for federal employees. The request is processed directly from the traveler's office to the contractor visit control office for clearance certification. Again, in all instances an independent computer or manual system is utilized to obtain the clearance information. Need-to-know certification signature level is less clear because contractors find it difficult to identify a management level that equates with the DOE Division Director. When questions arose, contractors lean toward a lower management level for certification. In some instances the management level selected is roughly equivalent to the DOE Branch Chief.

C.1.3 DOE Contractor Employees Where CVCS, Clearance Certification, and Visit Control Responsibility Has Not Been Delegated

This was by far the most inefficient process. The form, as is customary, is generated by the traveler's work section. It is then routed to the contractor's personnel security section for review. The contractor, after having verified the traveler's clearance status, routes the form to the visit control office of the DOE Field Office. The DOE visit control office again verifies, and certifies the traveler's clearance, and routes the form to the appropriate field office Division Director (or delegate) for the need-to-know certification signature. After signature, it is routed back to the DOE visit control office.

C.1.4 Need-to-know Signature for Outgoing Visits

Obtaining these signatures requires routing of the request form, which results in additional processing time. The delay was exaggerated when the individual(s) who are authorized to sign the form are not available. An additional grievance voiced by security personnel responsible for the program

was that there were occasions when unauthorized personnel signed the form (an administrative oversight) which resulted in "findings" during inspections and program evaluations.

Virtually all security personnel interviewed felt the current required signature level (Division Director) was too high, and many even questioned the need for a management signature at all. Signatures were usually being obtained to comply with the directive so that inspection "findings" could be avoided. While most managers would like to remain aware of which employees are working on certain programs and which are performing work-related travel, signing the visit request form is not an appropriate method to keep management informed. This could be accomplished with a listings of proposed travel for their review, but not approval. Similar to "Pending" incoming visit lists, CVCS should be capable of printing an "Outgoing" visit list.

Management and program implementors at all sites reviewed were asked to verbally justify the requirement for a management-level signature on the outgoing side of the process. In each instance, when confronted with various scenarios and arguments against the requirement (see below), they conceded that need-to-know was most appropriately the responsibility of the site being visited and that the ultimate responsibility is shouldered by the individual actually disclosing classified matter to the visitor.

Arguments Against Outgoing Need-To-Know Signature:

1. What has the signature accomplished when the visitor gains access to the site for a legitimate visit and then goes around visiting others, discussing unrelated programs and accessing classified matter? In these instances, which occur frequently, who determines need-to-know?
2. Why is there no management signature requirement when an employee, not on travel, goes to another activity, division or group to access classified matter?
3. In light of responses to the above, what individual is responsible for ensuring need-to-know? Is a signature necessary?

C.2 TRANSMITTAL OF THE REQUEST FOR CLASSIFIED VISIT

Once the form is returned to the visit control office, it is transmitted to the site being visited. The method of transmission is dependent upon two key issues:

1. Is the traveler requesting access to information that requires additional programmatic approval (e.g., weapons data or uranium enrichment information)?
2. Are the traveler's site and the site being visited both connected to the CVCS system?

In those instances when additional programmatic approval is required, the forms are transmitted via facsimile to the responsible program office (DP-23 for weapons data and NE-30 for uranium enrichment facilities and programs). It is the program office, not the site being visited, which finally approves the visit. If approved, the program office forwards the request to the visited site. The method of transmission is the computer system WDACS (Weapons Data Access Control System) for weapons data and facsimile for uranium enrichment information.

If no special programmatic access approval is required, and the involved sites are linked via CVCS, the request is entered into the CVCS system as a "pending" request and transmitted to the visited site. The visited site is responsible for approving or disapproving the visit.

If either of the two involved sites are not linked to the CVCS system, the primary method of transmittal is facsimile, followed by U.S. postal channels. There are times when both methods are used simultaneously.

Once the visit request has been transmitted, regardless of the manner of transmission (CVCS, facsimile, mail), information pertinent to the visit is entered into a local, redundant database. With the exception of one site, all

other sites reviewed maintain either a redundant computer database or a redundant manual system for classified visits. In those instances where CVCS is not extended to major contractors or outlying DOE sites, each separate entity maintains their own redundant computer database or manual filing system for the Classified Visits Program. All sites with redundant systems were queried about the need for such record-keeping. The predominant response was that separate local systems are maintained because CVCS is incomplete. Those offices keeping redundant databases incorrectly believed that CVCS only tracked requests transmitted between CVCS-linked sites and was not capable of keeping records of requests transmitted via other methods. Due to this incorrect assumption, they continue to maintain record systems that were in use prior to CVCS.

Data entry workload doubles for CVCS-transmitted visits to those sites linked to CVCS and that maintain redundant databases. The data is entered into CVCS for transmittal of a pending request, and the same information is again entered into the local system at the visited site.

For those DOE field offices which have not extended CVCS to major contractors or outlying sites, the data entry workload increases two to three times for CVCS-transmitted visits to contractors. In addition to CVCS, the contractors are keeping a separate database of classified visits, and the DOE field office is also keeping a redundant database.

C.3 INCOMING VISIT REQUESTS

Those issues that were encountered at both the outgoing site and the incoming visited site (or transmission between them) will be addressed in less detail because they have already been amply discussed in the previous sections. For example, maintaining redundant databases and the extra work it creates applies to both incoming and outgoing sides of the process. Because this issue was addressed in the Section C.2, it will only be briefly mentioned in this section.

The request is received at the visited site via one of three primary

methods (CVCS, facsimile or mail). However, once a hard copy request is in the hands of the visit control office at the visited site, requests are processed in the same manner.

C.3.1 CVCS Requests

Those sites linked to CVCS receive a "pending" visit request listing, usually on a daily basis. All sites complained that this pending list had to be manually compared with the previous day's listing. This was to determine which were new pending requests needing action versus pending requests already in the approval process but not yet approved.

Pending requests needing action are called up in the system and eventually printed so that a hard copy can be routed for "operational approval" signature. Printing the CVCS request screen is necessary because the DOE F 5631.20 form is not available in hard copy at the visited site for signature purposes.

Typically, the visit control office will telephone the point of contact to verify the visit and determine the level of access required. The data obtained is included in some manner on the form, and the form is routed to the individual having operational approval signature authority.

Routing the form for signature varied from site to site. At one site no signature was obtained, while at another signatures were obtained without contacting the point of contact to verify the need for the visit or the level of access. In those cases where the signature was obtained, it was again a matter of compliance rather than program integrity that motivated the process.

There are usually two primary purposes for signatures: one for authentication and the other for accountability. The latter probably applies in that someone will be held accountable should an unauthorized disclosure of classified matter be made. However, it should be noted that at some locations no signature is obtained, and at another site, after going to the trouble to obtain a signature, the form bearing the signature is discarded. Another

aspect of this issue is that the two persons most directly involved, the traveler and the host, never sign anything. Logic would dictate that the responsible individuals should be the accountable individuals; however, current procedures do not accommodate this.

When processing the form for signatures is completed, the CVCS request status is changed from pending to approved. One site was so far behind in pending visits (approximately 500) that it is not possible to process them in advance. They merely process the visitor when they arrive at the site.

C.3.2 Facsimile and Mail Requests

Classified visit requests received by facsimile or mail are processed the same as those received via CVCS with the exception that those received by facsimile or mail do not require approval within the CVCS system. The forms are routed for signature and the data entered into a local database.

C.3.3 Records

All paper copies of records are retained for five years. Again, all but one site reviewed maintained a separate and redundant database for incoming visits. The rationale was the usual--the perception that CVCS was incapable of maintaining information on visits not actually transferred via the CVCS system.

C.3.4 Programmatic Approval

The following deals with separate issues involving programmatic approval--specifically, approval to access weapons data, visits involving uranium enrichment programs or locations, and access to Sensitive Compartmented Information (SCI).

Weapons Data

The following does not pertain to those exemptions which exist for

visits within the weapons complex where programmatic access is pre-approved. When a non-weapons complex employee requests access to weapons data, DP-23 must approve the request (approximately 17,000 a year). Therefore, requests to access weapons data are not dispatched directly to the site being visited. Rather, the DOE F 5631.20 form is processed via facsimile to DP-23. DP-23 determines, through contact with both the visitor's and host's sites, the purpose for the access and the exact access required. DP-23 then passes the "approved" visit request to the visited site via the Weapons Data Access Control System (WDACS), a system totally independent of CVCS. WDACS is on-line through a modem to all 14 weapons complex facilities. However, similar to CVCS, the system does not alert the recipient when approved requests are passed. Since these are already approved requests, no further action is taken by the visited site in relation to contacting the host or obtaining "operational approval" signatures. If the visit is in WDACS, it is approved!

WDACS is updated at most connected facilities every week via some form of data transfer. Currently, listings of all visitors in the system are updated routinely. Some sites have even managed to accommodate WDACS by directly downloading data into their local system for badging purposes. This was a real advantage at one site.

If a WDACS-approved visitor arrives for a visit and the visit is not in the local system, the visit control office will review the WDACS hard copy listing. If a record of the visit request is not in the WDACS listing, they will check the on-line WDACS system. If it is not in the on-line system, they contact DP-23 via telephone. If it is an approved visit, DP-23 will forward the request to the visited site via facsimile and update WDACS.

A repeated complaint about the weapons data programmatic approval process is the time factor. Oftentimes DP-23 cannot respond quickly due to insufficient staffing.

Another problem was voiced about the signature authority required for other agency visitors to access weapons data. Some felt it was unnecessary to require such high-level signatures on the outgoing side of the process.

Uranium Enrichment

Uranium enrichment-related visits processed by NE-30 are far fewer than those processed by DP-23. NE-30 processes only about 300 to 500 per year. Programmatic approval requests are sent to NE-30 primarily by facsimile. The NE-30 approval process is similar to that of DP-23. After approving a visit request, NE-30 sends it to the visited site, mainly by facsimile.

Sensitive Compartmented Information (SCI)

The SCI access authorization program is administered for DOE within the Office of Intelligence (IN-40). DOE or DOE contractor personnel requiring access to SCI apply for access approval to a Special Security Office (SSO). Once individuals have met the additional clearance requirements, their clearance and SCI authorization are maintained by a local SSO.

Unlike the other two programmatic access approvals addressed above, SCI access authorization cannot be passed via the same means as used to pass security clearance information. SCI access authorizations can only be passed from SCI Facility (SCIF) to SCIF. Unlike other programs within DOE for passing clearances and programmatic accesses, there is no requirement for documentation. When one has been granted access to SCI, they merely instruct the SSO holding their access authorization to pass their authorization to the SCIF at the location they intend to visit. Typically the instruction to the SSO to pass the SCI access is accomplished verbally.

When the traveler arrives at the visited SCIF, positive identification is made and access granted. Need-to-know determinations are made separately from the process of passing the access authorization. Again, no documentation is required for a determination of need-to-know.

Current Process for Handling Classified Visits

APPENDIX D

RECOMMENDED PROCESS FOR DOE CLASSIFIED VISITS PROGRAM

APPENDIX D

RECOMMENDED PROCESS FOR DOE CLASSIFIED VISITS PROGRAM

The following steps comprise a procedure that we believe is both effective and efficient. The process is depicted graphically at the end of this appendix.

- Step 1: A cleared employee (subsequently referred to as "visitor") identifies the need to travel to another site and access classified matter. The visitor, working with the individual/company hosting the visit, determines travel requirements: 1) dates of visit and 2) access level needed to complete the work. It is during these initial, somewhat informal, interactions between the visitor and the host that initial justification is presented to demonstrate the visitor's need-to-know.
- Step 2: The visitor requests their local Security Office to pass their clearance to the Security Office of the visited site. The request to pass the visitor's clearance may come directly from the visitor. The visitor must provide certain information: 1) sufficient personal information, 2) name and location of the site to be visited, 3) identification of the person to be contacted at the visited site (host), 4) purpose of the visit, and 5) access required during the visit.
- Step 3: The visitor's Security Office certifies the visitor has a valid clearance and the level of clearance. This completed, the visitor's Security Office passes this information to the visited site. If the visitor requests access to data that requires additional programmatic approval (such as Weapons Data or Uranium Enrichment), the visitor's Security Office routes the classified visit request to the appropriate Headquarters program office

instead of the visited site. The program office then transmits its approval to the visited site.

- Step 4: Once the request is received at the visited site, the Security Office is responsible for contacting the host.^(c) Through the host, they will verify three things: 1) the necessity of the visit, 2) whether the visitor is expected, and 3) the level of access required during the visit. Based on input from the host, the visit is approved or disapproved. Unless desired, there is no need to have accountability outside the Security Office. This accomplished, the visit is approved or disapproved.
- Step 5: When the visitor arrives at the visited site, security personnel ensure the visitor is positively identified. Currently, picture identification is typically used. However, technologies such as biometrics can provide additional assurance of identification.
- Step 6: During the visit, it is the responsibility of the host to continually evaluate the visitor's need-to-know. Access to information for which the visitor does not demonstrate a need-to-know should be denied. Attempts to gain access to information outside the scope of the visit, without an adequately justified need-to-know, should be reported to Security.

(c) If programmatic approval is necessary, it is the program office that makes the contact rather than the Security Office at the visited site.

Recommended Process for Handling Classified Visits ³

- 1) This request can be accomplished informally (telephone/electronic mail) or more formally (a written form).
- 2) This verification can be by telephonic coordination documented by Security, or require a signature by the host.
- 3) While the traveler's management is not reflected as part of the above process, it must be noted that travel, and therefore any classified visit, does not occur without management awareness and concurrence in the form of a travel request and the obligation of funds.

APPENDIX E

REVIEW OF DEPARTMENT OF DEFENSE POLICY REGARDING CLASSIFIED VISITS

APPENDIX E

REVIEW OF DEPARTMENT OF DEFENSE POLICY REGARDING CLASSIFIED VISITS

Review of Department of Defense (DOD) directives^(d) disclosed the following guidelines pertaining to the their implementation of the Classified Visits Program:

- Advance notification (in writing) to the visited site is required.
- The visited site must approve the visit.
- A visit request will not be accepted from the visitor.
- Clearance certification will be accomplished by someone (other than the visitor) who is in a position to verify the visitor's clearance.
- The request must include: visitor's personal information, clearance information and employer information; identification of visited site; dates and duration of visit; purpose of visit in sufficient detail to determine need-to-know; and identification of personnel to be contacted at visited site.
- When no additional program access approval is required, need-to-know is determined by the individual responsible for disclosing the classified matter. In those cases when additional program access approval is required, the visit request is submitted to the responsible program office, which certifies the visitor's need-to-know. The request is then transmitted to the visited site by the program office.
- At the visited site, positive identification of the visitor is established prior to granting access.

(d) DOD 5200.1-R, Information Security Program. DOD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information.

- Records of classified visits will be retained for two years.

Site reviews disclosed that for the most part, DOE sites encountered few problems with military visitors. However, some sites reported dissatisfaction expressed by military visitors accessing Critical Nuclear Weapons Design Information (CNWDI). By DOD Directive 5210.2, only specific senior military command personnel can authorize access to Restricted Data and CNWDI. Such requests must bear the title block for one of the positions listed in the DOD directive. A delay is sometimes caused when the visit request must be returned because the appropriate title block is not on the request. It is interesting to note that as long as the form contains the appropriate "title," it can be signed by others.

One weapons complex contractor repeated a similar complaint voiced by visitors from the National Security Agency (NSA). Some visitors from this agency felt that visits were unnecessarily delayed because they did not have the proper position title typed on the form.

Since the majority of DOD visits concern access to restricted data, and primarily involve CNWDI (weapons data access), they are processed to and through DP-23. DOD requests can be processed directly to the visited site if the request deals with:

- Access to NSI.
- Access to Restricted Data that is not Weapons Data.
- Access to CNWDI for work that is "reimbursable."

DISTRIBUTION

No. of
Copies

OFFSITE

- 12 DOE/Office of Scientific
and Technical Information
- 25 A. B. Dalinsky, Chief
Personnel Security Policy Branch
Policy, Standards and
Analysis Division
Office of Safeguards & Security
U.S. Department of Energy
Washington, D.C. 20585
- D. A. Jones, Director
Policy, Standards and
Analysis Division
Office of Safeguards & Security
U.S. Department of Energy
Washington, D.C. 20585
- E. J. McCallum, Director
Office of Safeguards & Security
U.S. Department of Energy
Washington, D.C. 20585

No. of
Copies

ONSITE

DOE Richland Field Office
R. B. Goranson

- 29 Pacific Northwest Laboratory
M. H. Killinger (10)
S. W. Martin (5)
B. J. Merrill (5)
D. M. Montgomery (1)
M. A. Segura (2)
Technical Report Files (5)
Publishing Coordination

END

**DATE
FILMED**

8 / 25 / 92