MLM--3615

DE90 004826

Security Guide for Subcontractors

Prepared by Russell C. Adams,
Mound Security Education and Quality Audits

Issued: January 1990

MOUND

operated by
EG&G MOUND APPLIED TECHNOLOGIES
P.O. Box 3000, Miamisburg, Ohio 45343-3000

for the
U. S. DEPARTMENT OF ENERGY
Contract No. DE-AC04-88DP43495

CONTENTS

		Page
1.	Objectives	3
2.	Achievement of Objectives	3
3.	Responsibilities	3
4.	Physical Barriers	4
5.	Personnel Identification System	4
6.	Personnel and Vehicular Access Controls	6
7.	Classified Document Control	7
8.	Protecting Classified Matter in Use	7
9.	Storing Classified Matter	8
10.	Repository Combinations	8
11.	Violations	9
12.	Security Education	10
13.	Clearance Terminations	11
14.	Security Infractions	11
15.	Classified Information Nondisclosure Agreement	12
16.	Personnel Security Clearances	13
17.	Visitor Control	15
18.	Travel to Communist-Controlled or Sensitive Countries	16
19.	Shipment Security	16
20.	Surreptitious Listening Devices	17
21.	Additional Information	18
	Exhibit 1 - Sample Briefing - Initial Security Orientation	19
	Exhibit 2 - Sample Briefing - Comprehensive Orientation	25
	Exhibit 3 - Classified Information Nondisclosure Agreement	31
	Exhibit 4 - Data Report on Spouse	33
	Exhibit 5 - Security Termination Statement	35
	Exhibit 6 - Request for Visit or Access Approval	37
Index		39
Distribution		40

1. OBJECTIVES

The objectives of security in the Department of Energy (DOE) contractor/subcontractor program are:

- To protect information that, if released, would endanger the common defense and security of the nation.
- To safeguard plants and installations of the DOE and its contractors to prevent the interruption of research and production programs.

2. ACHIEVEMENT OF OBJECTIVES

To achieve security objectives, security responsibilities are divided into four interdependent categories: Personnel Security, Physical Security, Technical Security, and Security Education and Quality Audits.

Personnel Security determines whether DOE, contractor, and subcontractor personnel are eligible for security clearances and access to classified information.

Physical Security deters unauthorized access to installations, materials, and information and protects sites from sabotage, espionage, and theft.

Technical Security is responsible for the various security systems such as alarms, locks, and keys, as well as the DOE-required TEMPEST and technical surveillance countermeasures systems.

Security Education and Quality Audits develops and enforces procedures to control the dissemination of classified information and prevent its dissemination to unauthorized persons.

3. RESPONSIBILITIES

EG&G Mound Applied Technologies ensures security regulations are enforced at subcontractor facilities to protect DOE security interests connected with the Mound contract.

Subcontractors must comply with security directives, policies, and procedures issued by the DOE and Mound.

Employees involved in the DOE contractor/subcontractor program assume the following responsibilities:

- They must ensure the security of all classified matter entrusted to them.
- They must receive only classified information that they have a "need to know;" that is, the information required to perform their assigned duties effectively.
- They must report known or suspected security violations and infractions to the Mound security officer at (513) 865-3284.

- They must exercise discretion in responding to questionnaires or polls that might reveal classified information to unauthorized persons.

- They must adhere to all DOE regulations and procedures and all federal laws affecting national security.

Each subcontractor appoints a security officer and a classified document custodian for the facility. The security officer and the classified document custodian may be the same person. The security officer has the following responsibilities:

- Receive and disseminate DOE security instructions.

- Enforce security procedures.

- Give security orientations and instructions.

- Furnish the DOE with requested information regarding the facility security program.

- Notify Mound of any significant changes in facility status, such as a new security officer, a new document custodian, or a change of address.

- Obtain Mound approval prior to modifying security procedures or safeguards, unless modification is directed by the DOE.

- Provide Security Education with a letter of nonpossession for classified documents and materials at the completion of assigned contracts and purchase orders.

4. PHYSICAL BARRIERS

Access to security rooms and to repositories containing classified documents and/or material must be controlled by appropriately cleared personnel. (Personnel must have a clearance for access to material classified at or above the level of material being examined.) Access will be limited to cleared individuals who are on the access list and have a "need to know."

The security officer will issue keys to security rooms and combinations to repositories only to those cleared persons whose duties require that they have the keys and/or combinations. Access lists to security rooms and safes should be posted on the doors or safes as appropriate. A record of all locks, cores, and keys to security rooms or repositories must be maintained. Locks will be changed or recored every five years, when a key is lost, when a key or lock has been compromised, or when unrecorded keys are found. Terminating personnel will turn in their keys. A physical inventory of locks, keys, and cores will be conducted at least annually, and immediate action will be taken to replace or recore locks for which keys are missing or for which unrecorded keys are found.

5. PERSONNEL IDENTIFICATION SYSTEM

A security badge or pass system will be used to ensure that only authorized personnel enter, occupy, and leave a security area and to indicate limits on

access to classified materials. This system will be used to control access to security areas in which 30 or more persons work; however, personal recognition may be used to control access to security areas in which fewer than 30 persons are employed.

Employees and visitors within a security area will prominently display the badge or pass required for entry. It will be worn above the waist unless prohibited by health or safety regulations.

Badges or passes for visitors will bear, as a minimum, the following data:

- Escorted visitors: the visitor's name, a serial number, the period of the visit, and an indication that an escort is required. If the visitor is a foreign national (a citizen of a foreign country), this should be indicated on the badge.

- Unescorted visitors: the visitor's name, type of access authorization, security areas the visitor may enter if appropriate, and expiration date. Badges that are not removed from the site need to show only a serial number, type of access authorization, security clearance, or areas to which the visitor is permitted or allowed unescorted access.

Badges or passes for employees will be tamper-resistant. The front will display the name and location of the issuing office, the contractor or subcontractor, the employee's name, a clear, full-face photograph of the employee large enough for easy identification, and a serial number. Additional information may include a personal description, the signature of the holder, and the signature (or facsimile) of the issuing official. Coding indicating categories of information the employee has access to, areas within the facility the employee may enter, or the degree of access authorization may also be included.

Temporary employees will be issued badges or passes conforming to the same requirements as badges for permanent employees.

Badges and passes for permanent employees must meet the following specifications:

- The photograph dimensions, exclusive of the name, will be at least 1½ inches long by 1¼ inches wide, and the facial image will be as large as practicable within these limits.

- The face of the insert or the bonding material will contain an ink or dye noticeably affected by the heat, erasure, or solvent necessary to relaminate, remake, or alter the badge. (Fluorescent inks or dyes, magnetized matter, water marks, superimposed cross threads or wire, or other material designed to prevent fraud may be used.)

- Inserts will be laminated between sheets of transparent plastic so that the plastic bonds together securely and completely covers the insert.

- All badge inserts will be serially numbered, and strict accountability and control of plates and inserts, including those scrapped or damaged, will be maintained.

Badges and passes for permanent employees may be manufactured to specifications other than those set forth above, provided the degree of tamper resistance is equivalent to or greater than that specified.

Records showing the disposition of all badges and passes will be maintained. They will include the date of issue, name of holder, type of access authorization, and, if applicable, the categories of information and the areas within the facility to which access is authorized.

A record of lost badges and passes will be kept, and personnel controlling access to security areas will be notified of any lost badges to prevent their misuse.

Stocks of inserts and unissued badges and passes will be stored to prevent loss, theft, or unauthorized use. At a minimum, they will be stored in a manner approved for storing Confidential matter.

Terminating employees will turn in their badges and passes. Visitors will return badges and passes at the conclusion of each visit.

Badges and passes issued to permanent employees will be replaced by new badges with a different background design or color and new photographs when 5% of the badges in use have been lost, or at least every five years.

If the facial appearance of an employee changes significantly, a badge or pass with a new photograph will be issued.

6. PERSONNEL AND VEHICULAR ACCESS CONTROLS

The identity of persons authorized access to a security area will be verified at the entrance by a protective force member, receptionist, or other authorized person. Remote identification by television may be used, provided positive identification is ensured. Also, an unattended mechanical or electrical admittance system may be used at an inner security area (i.e., an area within a larger security area).

Security area entrances and exits will be equipped with doors, gates, rails, or other movable barriers to direct and control the movement of personnel or vehicles through designated posts.

A visitor log will be maintained to record the name, signature, organization, and citizenship of each uncleared visitor to a security area; the names of persons visited; escort names and signatures; purpose of visit; and time in to and out of the security area.

A visitor without appropriate access authorization will be escorted at all times while within a security area. The escort may be a protective force member, the person being visited, or other designated employee.

7. CLASSIFIED DOCUMENT CONTROL

The classified document custodian will maintain strict accountability for all classified documents received or generated.

DOE Order 5635.1A furnishes complete and detailed information concerning marking and handling classified documents. Contact Mound Security ((513) 865-3284) for additional information.

Only personnel with "Q" access authorizations may have access to Secret Restricted Data. Personnel with "L" access authorizations may have access to Confidential Restricted Data or Secret National Security Information.

All mail sent to the subcontractor's classified mailing address will be delivered unopened to the security officer. If a package shows evidence of tampering, notify Mound Security immediately ((513) 865-3284).

Custodians must ensure that all classified documents are locked in a repository at the close of business each day.

When no longer needed, classified documents (including drafts and work sheets) connected with Mound interests will be returned to Mound (Confidential by first class certified mail; Secret by first class registered mail). The approved Mound classified mailing address is given in section 19.

Secret documents should be audited annually against the accountability records. When a classified document is unaccounted for at a subcontractor's plant and there is no indication that federal law has been violated, the security officer will notify the manager, Mound Security.

> Note: Offsite losses of classified documents or material and onsite losses indicating a violation of federal law are covered in section 11 of this guide.

8. PROTECTING CLASSIFIED MATTER IN USE

Classified matter (documents or materials) will not be removed from a security area without authorization.

Classified matter in use will be constantly attended by, or under the control of, appropriately cleared personnel concerned with its use. (Personnel must have a clearance for access to material classified at or above the level of material being examined.)

Persons attending or controlling classified matter will prevent access to the material by unauthorized personnel. This includes preventing unauthorized visual access when classified information may be obtained by observing the material.

An accountability system will be maintained to promptly reveal the loss or unaccountability of classified matter. Secret classified material should be audited annually against the accountability records. Actions will be taken to recover the material or to ascertain the disposition of matter that cannot be located. Discrepancies between records and materials on hand must be resolved.

Classified material and equipment will bear classification identification (level and category) and extra markings such as stamps, tags, or labels.

Any classified matter that is lost or cannot be accounted for will be reported promptly to Mound Security ((513) 865-3284), which will issue additional instructions.

9. STORING CLASSIFIED MATTER

When not in use, classified matter must be attended by a cleared employee or stored in a locked repository approved for storing classified material by the DOE or the Mound security auditor who surveyed the facility. If operating requirements indicate the need for additional or substitute repositories, the manager, Mound Security, should be contacted for approval.

A monitor sheet (standard form 702, Security Container Check Sheet) will be posted on each repository containing classified matter. This sheet will be initialed at the end of each workday by the person who locks the repository and by one other person who checks the lock, locked door or drawer, and all exposed drawers to ensure the repository is properly secured.

10. REPOSITORY COMBINATIONS

The combination to a repository may be revealed only to cleared personnel who are authorized access to the classified matter. The repository combination will be changed:

- When the repository is placed in use after procurement.
- When a person who knows the combination terminates employment or no longer requires access to the repository.
- When the combination has been subjected to compromise.
- At least once every 12 months.

Records of repository combinations will be classified no lower than the highest classification of the matter stored in the repository.

The date of the most recent combination change will be posted on the repository.

The Security Container Information Form, SF-700, will be used on all security containers, approved rooms or vaults, and other locations where classified

matter is stored. SF-700 should be filled out according to the instructions on the form, with two exceptions:

- Part 1 of SF-700 will be affixed to repositories to ensure high visibility. In rooms or vaults, part 1 will be affixed to the inside of the door containing the combination lock. On safes, it will be placed on the inside or the front of the locking drawer at the user's discretion.

- Part 2A should not be completed. If the combination is recorded in this section, the form must be classified at the highest classification of information stored in the repository.

If an unattended repository containing classified matter is found open, one of the custodians should be notified immediately, the repository should be secured by a designated person (e.g., a guard or watchman), and the contents should be checked no later than the next workday.

11. VIOLATIONS

Violations include the following:

- Alleged or suspected criminal violations of the Atomic Energy Act of 1954; the Internal Security Act of 1950 relating to DOE projects; Title 18 of the U.S. Code relating to espionage or information control, sabotage, treason, subversive activity, and malicious mischief; and other federal statutes that may be enacted relating to the security of DOE projects, activities, facilities, and classified information.

- Onsite loss of classified matter under circumstances indicating a violation of law.

- Offsite loss of classified matter even if no violations of federal law are indicated.

- Onsite loss of classified matter if there is no immediate explanation for the loss, even if no violations of federal law are indicated.

- Theft, illegal possession, and unlawful destruction or use of government property.

When an incident occurs that facility personnel believe is a violation, they will immediately telephone one of the following persons:

Name	Office Phone	Home Phone
Daniel L. Baker Manager, Security	(513) 865-4282	(513) 277-0789
Clyde W. Taylor Quality & Audits Supervisor	(513) 865-3284	(513) 424-5032

The person contacted will determine whether the circumstances indicate a violation and will provide further instructions to facility personnel. If the

above persons cannot be contacted promptly, the nearest office of the Federal Bureau of Investigation will be notified, and one of the above persons will be contacted as soon as possible.

12. SECURITY EDUCATION

The facility security officer develops and maintains a security education program to ensure that all personnel fully understand their security responsibilities.

12.1. Orientation

Employees granted access authorizations will be informed of their security responsibilities and applicable security regulations before they are given access to classified information. This will be accomplished by an initial briefing followed within 30 days by a more detailed and comprehensive orientation. (See sample briefings, Exhibits 1 and 2.) However, if circumstances require that an employee's security orientation be completed in one session, the comprehensive orientation will be given.

The initial security briefing will include, as a minimum, the following topics:

- United States policy regarding the development, use, and control of atomic energy.
- Definition of Restricted Data, Formerly Restricted Data, and other National Security Information.
- The need and responsibility to protect classified material; the "need-to-know" principle.
- Federal laws applicable to unauthorized disclosure of classified information.
- Security areas, purpose and use of employee badge (if applicable), parts of facility to which employee is authorized access, and prohibited articles.
- DOE drug program.

The comprehensive orientation will include, as a minimum, the following topics:

- Purpose of the DOE security program.
- Legal basis for the DOE security program.
- Responsibility for protecting classified information and complying with security regulations.
- Duties of supervisors and their employees in safeguarding classified information.

- Components of the security program and their relationship.
- The keystone of the security system.
- Threats to security.
- Employee responsibility to report threats to security.
- Reporting arrests and changes in marital status.
- Bomb threats.

12.2. Continuing Security Education

Continuing security education will be conducted to ensure employees are kept apprised of their security responsibility. This continuing education will include the use of visual aids, conferences, staff meetings, lectures, and on-the-job training.

All cleared employees will receive an annual refresher lecture to remind them of their continuing security responsibilities, and on-the-job security training will be conducted as necessary.

All employees will be informed of new and revised security regulations and instructions pertaining to their security responsibilities. The Mound Security section will periodically furnish posters, pamphlets, and other visual aids to employees.

12.3. Records

Records of security lectures will be maintained. They will include the type of lecture (i.e., initial, comprehensive, periodic refresher, etc.), date, time allotted, and list of attendees.

13. CLEARANCE TERMINATIONS

All employees with access to classified information will be advised of their continuing security responsibilities upon termination of their clearance. See section 16 of this guide for further instructions regarding terminating employees.

14. SECURITY INFRACTIONS

A security infraction is an act or omission involving failure to comply with DOE regulations for protecting classified information or material. DOE and Mound security regulations are to be observed by all employees. Security infractions must be held to an absolute minimum, and, after an infraction, necessary actions will be taken to preclude recurrence.

The following examples illustrate various types of security infractions:

- Leaving classified documents or material exposed and unattended or unsecured at the close of business or when a room is unattended.

- Storing classified documents or material improperly.
- Failing to safeguard or account for classified documents or material, which results in the matter being unaccounted for or compromised.
- Failing to maintain prescribed records for Top Secret or Secret documents.
- Removing classified documents or material from a security area without proper authorization.
- Failing to mark a document properly after its classification has been determined.
- Failing to obtain classification guidance, thereby compromising classified information.
- Changing the classification of documents without proper authorization.
- Failing to properly safeguard repository combinations.
- Destroying classified documents improperly.
- Transmitting classified documents or material improperly.
- Discussing classified information in the presence of unauthorized persons.
- Discussing classified information over standard telephone systems.
- Failing to escort uncleared visitors in security areas.
- Permitting an unauthorized person to hear, see, or otherwise obtain classified information.

The security officer and the supervisor of the person who committed the infraction will take actions necessary to prevent a recurrence of the infraction.

Appropriate discipline of employees responsible for security infractions is encouraged. The circumstances of the infraction should determine the severity of the disciplinary action.

The security officer must promptly notify the manager, Mound Security, by telephone of all security infractions. This must be followed by a complete written report that specifies corrective and disciplinary actions taken.

15. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

To comply with DOE Directive 5631.1A (Safeguards and Security Awareness Program), all employees granted a Q-clearance access authorization will be given an orientation by Security on the Classified Information Nondisclosure Agreement, standard form 312 (see Exhibit 3). Applicable sections of

federal statutes concerning the Atomic Energy Act of 1954, U. S. Code (Titles 18 and 50), National Security Information Executive Order 12356, and the Intelligence Identities Protection Act of 1982 will be made available to all individuals before they sign the agreement. After reviewing the statutes and attending the orientation, each Q-cleared individual will be required to complete and sign the Classified Information Nondisclosure Agreement. This form must be completed before an employee is given access to classified matter. This form will be witnessed and signed by the security officer of the subcontractor organization, then promptly mailed to the Mound Security Education supervisor for forwarding to DOE/Albuquerque (AL).

16. PERSONNEL SECURITY CLEARANCES

Subcontractors performing classified work for the DOE must establish and maintain a preemployment check program to eliminate background security investigations of individuals who are obviously unqualified or unsuitable for employment. Before a request for access authorization (clearance) is submitted, the subcontractor should contact references, former employers, and educational institutions to ascertain the applicant's general suitability for employment, including reliability, integrity, and personal habits. Preemployment checks should not inquire into matters of loyalty or associations of a subversive nature, but should be confined to matters of character and employment desirability.

Any increase in the number of active access authorizations must be justified by programmatic needs. If a subcontractor needs additional access authorizations, adequate justification must be submitted to Mound. Mound Visitor Control will furnish the instructions for preparing the forms required to process clearance requests.

All inquiries concerning the status of access authorizations should be made to the Mound Personnel Security office at (513) 865-3272.

If an employee whose access authorization is being processed no longer requires a clearance, the Mound Personnel Security office must be notified by telephone ((513) 865-3272) or facsimile ((513) 865-5173) so that the investigation may be discontinued.

Persons who marry after applying for an access authorization must complete form DOE F 5631.34 (Exhibit 4), in duplicate, and submit it to Mound Visitor Control. This form is also required for applicants for clearance who are married to foreign nationals.

Mound will notify the subcontractor security officer when access authorizations are granted. Prior to being given access to classified matter, persons granted a clearance must be given a security orientation briefing and must sign the Classified Information Nondisclosure Agreement (see sections 12.1 and 15.)

The Mound Security section should be informed when persons terminate their employment to enter the armed forces. The DOE notifies the Department of Defense (DOD) when persons who have had access to classified information of current importance to DOE programs are called to active duty. This provides

the DOD with information to be considered in assigning responsibilities to these individuals. This provision also applies for persons who assume active duty any time after terminating employment.

If it is determined that an employee holding or being processed for a Q or L access authorization may have a mental illness that could adversely affect judgment or reliability, or if an employee has committed suicide, has attempted suicide, or is a missing person in that his whereabouts are unknown to his family, employer, or associates, the subcontractor security officer will promptly notify the Mound Personnel Security supervisor at (513) 865-3272. The Personnel Security supervisor will advise the security officer of the actions to take and the DOE reporting requirements.

All supervisors must promptly report to the security officer (without benefit of opinion or confirmation of validity) derogatory information concerning applicants for access authorizations and employees who have access authorizations. The security officer must relay these reports immediately to Mound Personnel Security at (513) 865-3272. Derogatory information includes, but is not limited to, questionable loyalty, association with persons of questionable loyalty, illegal drug use, alcoholism, dishonesty, noncompliance with security regulations, sexual perversions, and arrests (even if charges were dismissed). Minor traffic violations for which a fine of $100.00 or less is imposed (not including court costs) do not need to be reported. Any notice of financial irresponsibility is also to be reported; e.g., bankruptcy, garnishment, repossession of motor vehicle, and lawsuit judgments.

All personnel holding access authorizations should promptly notify the security officer of any direct or implied threats against the President of the United States or any high-ranking government official. The facility security officer will in turn notify the manager, Mound Security, at (513) 865-4282.

The DOE requires personnel possessing access authorizations to be reinvestigated at stated intervals. This allows personnel security records to reflect a reasonably current status on an individual's background, character, associates, and loyalty. To facilitate these reinvestigations, Mound will periodically ask the security officer to furnish Questionnaires for Sensitive Positions for selected facility personnel. These questionnaires should be completed and returned to Mound Visitor Control by the date requested.

When an individual holding an active access authorization terminates employment, completes the assignment, or no longer requires access to classified data, his access authorization must be <u>immediately</u> terminated. At the time of termination, the security officer must remind the terminating employee of his continuing security responsibilities under existing federal statutes.

A signed copy of the Security Termination Statement, form DOE F 5631.29 (Exhibit 5), witnessed by the security officer, must be immediately forwarded to Mound Personnel Security with a letter including the employee's name, position, reason for termination, effective date, home address, and, if known, next place of employment. If an employee refuses to sign the Security Termination Statement, the security officer should explain the purpose of the form and the employee's obligation to sign it. If the employee continues to refuse, the security officer should find out the reason. If this approach is

unsuccessful, the Mound Security Education and Quality Audits supervisor will be contacted immediately by phone ((513) 865-3284) to provide guidance for further actions.

A report of the termination circumstances will be furnished to Mound Personnel Security if a cleared employee is discharged or permitted to resign for a cause reflecting on his integrity.

The security officer will ensure terminating employees return all classified documents and material charged to them.

17. VISITOR CONTROL

Visits to a subcontractor facility and visits by subcontractor personnel to other facilities to obtain classified information must be controlled to ensure that personnel have access only to the classified information they have a "need to know" and that they have appropriate access authorizations. Only those visitors approved by Mound may have access to classified matter relating to Mound projects. All approvals will be signed by Daniel Baker, manager, Security; Mike Shade, special projects manager; and Rita Krasnonski, Personnel Security supervisor. Usually, requests for visits and access approval will be made using form DOE F 5631.20, Request for Visit or Access Approval (Exhibit 6).

Form DOE F 5631.20 will be completed and forwarded to a subcontractor facility prior to a visit by cleared Mound employees. Visits by cleared personnel from a subcontractor facility to Mound do not require this form. Such visits should be arranged by telephone.

If subcontractor personnel must visit other facilities to discuss classified information concerning Mound work, a written request and justification for the visit should be submitted to Mound Personnel Security. Mound will arrange for the visit and retain a copy of completed form DOE F 5631.20 on file. Visit requests will normally be addressed to the Mound Security section. Approved forms will be forwarded to the subcontractor for permanent retention as access authorization for the visitor. Any of these forms sent directly to a contractor should be forwarded to Mound Visitor Control for processing. The contractor will not allow the visitor access until the visit is approved by Mound.

All visitors should be positively identified, and access to classified information must be limited to that requested. The subcontractor will maintain a permanent log of all visitors afforded access to classified information. The log will show the time and date of the visit, the name and citizenship of the visitor, the purpose of the visit, and the name of the person authorizing the visit.

Uncleared individuals may enter security areas only when all classified documents and materials are secured in approved repositories or containers. Foreign nationals are not allowed in security area without prior written approval from Mound.

18. TRAVEL TO COMMUNIST-CONTROLLED OR SENSITIVE COUNTRIES

With the exception of travel to Canada and Mexico, any impending visits to foreign countries must be reported to Mound Security. Mound personnel will then determine the status of the country. (An active list is on file in the Mound Security Education office.)

Security clearances will be terminated (without prejudice to reinstatement) when foreign travel is to extend longer than three months and is not in connection with official government business.

19. SHIPMENT SECURITY

Prior to each shipment of classified material, the recipient should be notified (information should include date, protective service, weight, waybill number, number of containers, and estimated time of arrival).

For subcontractors authorized to ship classified material, the approved shipping address for Mound is:

EG&G Mound Applied Technologies
Mound Road
Building 61, Room 112
For: (Intended Recipient)
Miamisburg, Ohio 45342

The notification address is:

EG&G Mound Applied Technologies
P.O. Box 3000
Miamisburg, Ohio 45343-3000
Attn: Arthur Heitkamp, supervisor, Traffic,
or Cindy Fuller
Telephone: (513) 865-3257 or (513) 865-3560

The approved Mound mailing address for classified material is:

EG&G Mound Applied Technologies
Attn: Document Control
P.O. Box 3000
Miamisburg, Ohio 45343-3000

Secret and Confidential documents will be enclosed in two opaque envelopes or wrappers for mailing. The classification markings on the inner envelope must not be visible through the outer envelope, and the contents of a classified document must not be visible through the inner envelope.

The inner envelope or wrapper will be addressed to the intended document recipient. The address is to be approved for classified mail. The level of classification must be placed at the top and bottom on both the front and back of the inner envelope.

If documents bearing different levels of classification are transmitted in the same envelope or wrapper, the marking on the envelope will match that of the document with the highest classification.

The classification category, i.e., Restricted Data, Formerly Restricted Data, or National Security Information, must be on the front of the inner envelope or wrapper.

The outer envelope or wrapper will be sealed with fiber-reinforced tape and addressed in the ordinary manner. There should be no indication on the envelope that the contents are classified. The sender's approved return address for classified material will also be shown on the outer envelope.

Secret documents must be sent by registered first class mail only. Confidential documents must be sent by certified first class mail.

If the envelope or wrapper used to transmit classified documents shows any evidence of tampering, the recipient will preserve the parcel as received and contact Mound Security ((513) 865-3284) for instructions.

Packages containing classified material will be banded in at least two directions with steel strapping and secured with distinctive DOE/AL seals. A notched banding will be used. The AL security seals will be obtained from Mound. They will be protected to prevent use by unauthorized persons. Used seals will be mutilated to prevent reuse.

Packages of classified material will include a card or other notice that will immediately alert receiving personnel of the classification of the material.

Shipping containers will be inspected immediately upon arrival. If the container, seal, or banding is broken, or if any other evidence of tampering is present, the Mound Security section will be notified immediately.

20. SURREPTITIOUS LISTENING DEVICES

If a suspected surreptitious listening device is discovered in the facility, it should not be tampered with, moved, or altered. One of the following persons should be notified immediately:

Name	Office Phone	Home Phone
Kevin N. Gardner Technical Security Supervisor	(513) 865-3583	(513) 433-7420
Paul D. Collins Security Technician	(513) 865-3596	(513) 746-5077

21. ADDITIONAL INFORMATION

Requests for clarification of this security guide and questions on security matters should be addressed to:

D. L. Baker, Manager, Security
EG&G Mound Applied Technologies
P.O. Box 3000
Miamisburg, Ohio 45343-3000
Telephone: (513) 865-4282

SAMPLE BRIEFING

INITIAL SECURITY ORIENTATION

The purpose of this meeting is to present for you an initial security orientation briefly covering several topics of security significance. Within 30 days you will attend a more comprehensive orientation, and at that time we will cover these and several other topics in greater detail.

We administer a classified contract for EG&G Mound Applied Technologies and the Department of Energy and, therefore, Title 18 of the U.S. Code, the Internal Security Act, and various executive orders apply to our cleared employees. Briefly, these regulations provide severe penalties for the unauthorized disclosure of classified information. Section 798, Title 18, U.S. Code, specifically states, "Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information . . . shall be fined from $10,000 to $20,000, or imprisoned from ten years to life, or a combination of both. In some cases, the death penalty may apply."

The term "classified information" describes information that has been determined to require special safeguards in the interest of national defense. Classified information is divided into three classification groups: Confidential, Secret, and Top Secret, in ascending order of importance. Classification is determined by the degree of harm that could result to the United States if that information fell into enemy hands. Classified information is further categorized as Restricted Data, Formerly Restricted Data, or National Security Information. The Restricted Data marking identifies data concerning the following: the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy.

Formerly Restricted Data is classified information that relates primarily to the military utilization of atomic weapons and has thus been removed by DOE from the Restricted Data category.

The National Security Information marking identifies classified information not included in the categories of Restricted Data or Formerly Restricted Data.

The policy of DOE, as stated in the Atomic Energy Act of 1954, is to control the dissemination and declassification of Restricted Data to protect the common defense and security. Until effective, enforceable international safeguards against the use of atomic energy for destructive purposes are established by an international arrangement, there will be no exchange of Restricted Data with other nations except as authorized by the DOE.

The dissemination of unclassified scientific and technical information relating to atomic energy is encouraged to enhance the free interchange of ideas and criticism that is essential to scientific and industrial progress and public understanding.

Based on the "need-to-know" principle, you will be granted access to classified information, up to and including Secret, that is required to perform your job. Access to classified information or material carries with it the responsibility for its protection. We must not overlook the fact that the technical expertise necessary to devise nuclear weapon systems can be found in practically every nation. Therefore, it is essential that we safeguard the classified technology we possess to remain ahead of our potential enemies.

Mound utilizes three basic types of security control: access control, physical control, and, the most important, individual control. Now, let's look at access control.

The first step in access control is to obtain an access authorization or security clearance. Generally speaking, there are two types of access authorizations. The first is an "L" access authorization, or "L" clearance. This grants limited access up through the level of Confidential only. It is based on certain national agency checks, such as the files of the FBI, CIA, and the House Committee on Un-American Activities. The other type of access authorization is the "Q" access authorization, or "Q" clearance. This is based on the same national agency check, plus an extensive background investigation made by the U.S. Office of Personnel Management and, in some cases, the FBI. You are subject to reinvestigation at least every five years.

To keep your access authorization current, you are requested to report personal information to the security officer. This data will be forwarded to DOE. First, report any derogatory information. This includes all arrests, charges, and detentions that are imposed upon you by law enforcement agencies, regardless of the circumstances. There is one exception: minor traffic offenses for which a fine of $100 or less (excluding court costs) is imposed do not have to be reported.

Secondly, report any changes in your marital status. If you marry, remarry, or are married to a foreign national, this should be reported. You will be asked to fill out a Data Report on Spouse form, and it will be forwarded to DOE. This is required because your spouse must also be investigated. Any changes in your military status (if you're called to active duty as a result of enlistment, induction, reserve callup, etc.) should also be reported.

Third, if you plan to travel to a sensitive or communist-controlled country, you are requested to notify Security of such plans at least 60 days prior to your departure. This is a continuing requirement, even after you terminate your employment. Normally, no restrictions are imposed on such travel unless, of course, your access to classified information will in some way endanger you or the DOE program.

There are a several additional items you are requested to report. First, report any mental instability observed in another Q-cleared person. Mental illness may seriously affect judgment or reliability. Also, report any direct

or implied threat to the President of the United States or other high officials in the U.S. government.

You must notify Mound Security of any approaches or contacts by organizations or individuals of any nationality, including U.S. citizens, either within or outside the scope of their official activities, in which illegal or unauthorized access is sought to classified or sensitive information, technology, or special nuclear materials or in which the individual believes he may be the target of an attempted exploitation by a foreign entity.

Additionally, you must report any unofficial contact with organizations or individuals from Communist Bloc countries.

You must also notify Mound Security of actual or imminent security incidents, such as the compromise of classified information, acts of sabotage or terrorism, or approaches or contacts by hostile intelligence organizations.

Let's talk briefly now about physical control. *(Briefly explain the security areas of the facility and how access to these areas is controlled.)*

As I said earlier, the most important control is individual control because, in the final analysis, access control and physical control rely upon the individual. Our system of controls provides us with "security in depth." We have physical barriers such as fences, guards, alarms, and safes. We have access controls: "Q" clearances and our badges. Although these are interdependent, they all depend upon the individual. They would be of little use if we, as individuals, were remiss in our duties and responsibilities toward security.

Now, the question is, how do we control and handle classified matter? In order to do this, you must be able to recognize classified matter. Classified matter exists in two forms: documents and material. Remember, of course, that oral discussions of classified information must be carefully guarded to ensure they are not overheard by unauthorized persons.

Documents consist of any recorded information. It can be handwritten or typed. It can be a film, a rough draft, a tape recording, a photograph, etc. If it is recorded information, it constitutes a document.

Material, on the other hand, refers to certain physical items, such as assemblies, components, tools, and gauges.

The basic rule is the same for both documents and material. Classified matter must be in the custody of a properly cleared individual, or it must be secured in an approved repository.

What about infractions and violations? An infraction, by definition, is the failure to comply with established DOE security regulations. Examples are leaving a safe open and unattended, leaving a document unattended, or improperly escorting an uncleared visitor. You will become more familiar with these regulations in time.

A violation is much more serious. This involves criminal violation of federal laws covering such things as sabotage, espionage, treason, malicious mischief, and other subversive activities. Violations are investigated solely by the FBI, and a person convicted of a violation could receive fines, imprisonment and, possibly, the death penalty.

It's important that you know the difference between infractions and violations. A good way to remember them is that infractions are usually committed as the result of carelessness or negligence. Violations are usually committed intentionally. However, it is possible to commit a violation through carelessness.

In this regard, we ask that you be very wary of surveys, which could lead to an unauthorized disclosure of classified information. If you receive a telephone survey asking pertinent questions about your relationship with Mound, refuse to answer and hang up. If you receive a questionnaire through the mail with questions as to how many people work here, types of operations performed, etc., please bring it in to us first so we can check its validity.

Also, neither confirm nor deny. This refers to classified information or information that you may consider classified when published in various news media. The publication of such information does not mean that it has been declassified. You are still obligated to maintain secrecy. If someone asks you whether it's true or false, you should say that you have no comment on the matter, or you might say "I don't know." Sometimes you can deny the truth of classified information and, at the same time, reveal a certain amount.

Finally, report suspicious persons. If anyone seems overly inquisitive about you or our classified work, please report them.

It is very important to avoid loose talk at all times, mainly because privacy is a thing of the past in 20th-century America. I say that because, in recent years, numerous surreptitious listening devices have been developed, many of which are sophisticated and miniaturized to a point where they are difficult to detect. It is a violation of federal law to use a surreptitious device to obtain information without the consent of the parties involved. The presence or installation of such a device is prohibited in DOE facilities. However, if you discover what you suspect to be a surreptitious listening device, notify the security officer immediately. Do not leave the device unattended or permit it to be moved, altered, or tampered with until the security officer arrives.

You should never engage in classified conversation at home, while riding in a car, on the phone (either in the plant or at home), or in any situation where the conversation could be overheard by an unauthorized person.

Additional topics or explanations unique to a given facility should be covered as deemed appropriate. They should include as a minimum the following:

1. *Security areas of the facility.*

2. *Areas to which the employee will have access.*

3. *Use of the employee's badge (if applicable).*

4. *Articles prohibited in the facility; i.e., alcohol and alcoholic beverages, illegal drugs, cameras, copying or reproduction devices, recording devices, radio transmitters, firearms, explosives, incendiary devices, and other articles that may be used to record, transmit, or reproduce classified information surreptitiously or to cause property damage or injury.*

5. *Other local restrictions.*

6. *The insider threat. By definition, the insider threat is a cleared individual working independently or in conjunction with one or more persons on the outside whose prime objective is to seriously damage DOE programs or property. This may include theft of classified parts or documents, sabotage of critical equipment or work areas, or any other damage that could give an advantage to our enemies. Employees, by observing and being aware of personnel in their work areas or unusual happenings around them, can be instrumental in defeating this serious threat.*

EXHIBIT 2

SAMPLE BRIEFING

COMPREHENSIVE ORIENTATION

During this phase of your security education, we will take a more comprehensive look at the Department of Energy's security program and how we implement DOE security guidance.

Why DOE Has a Security Program

The Atomic Energy Act of 1954 establishes the basis for our security program. The act sets forth the policy of the United States to direct the development, use, and control of atomic energy to make the maximum contribution to the general welfare. This is subject at all times to the paramount objective of making the maximum contribution to the common defense and security. Our security profile is intended to provide the necessary safeguards to ensure the implementation of this policy.

You should recall from your initial orientation that much of the information pertaining to DOE programs is classified and that classified information in any form must be protected in the interest of national defense. Classified information is divided into three classification groups: Confidential, Secret, and Top Secret, in order of ascending importance. They are differentiated by the degree of harm that could result to the United States if the information fell into enemy hands. Classified information is further categorized as Restricted Data, Formerly Restricted Data, or National Security Information. The Restricted Data marking identifies data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear materials; or the use of special nuclear material in the production of energy.

Formerly Restricted Data is classified information that relates primarily to the military utilization of atomic weapons and has thus been removed by DOE from the Restricted Data category. The National Security Information marking identifies classified information not included in the categories of Restricted Data or Formerly Restricted Data.

Unclassified Controlled Nuclear Information (UCNI) is a category of unclassified information. The UCNI marking limits the distribution of a document, as not all cleared individuals have access to information in this category.

The policy of DOE, as stated in the Atomic Energy Act of 1954, is to control the dissemination and declassification of Restricted Data to protect the common defense and security. Until effective and enforceable international safeguards against the use of atomic energy are established, there will be no exchange of Restricted Data with other nations, except as authorized by the DOE.

The Legal Basis for the DOE Security Program

The provisions of the Atomic Energy Act of 1954, the Espionage Act, Title 18 of the U.S. Code, the Internal Security Act, and various executive orders apply to each of us and provide the legal basis for the DOE security program. Briefly, these regulations provide severe penalties for the unauthorized disclosure of classified information. Section 798, Title 18, U.S. Code, specifically states, "Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information . . . shall be fined from $10,000 to $20,000, imprisoned from 10 years to life, or a combination of both. In some cases the death penalty may apply."

Responsibility for Protecting Classified Information and Complying with Security Regulations

Based on the "need-to-know" principle, you will be granted access to classified information, up to and including Secret, that you require to perform your job. Each of us is responsible for safeguarding all classified information to which we have access. It is essential that such information be identified and marked with the proper classification markings when it is originated.

As you become more familiar with these and other security procedures, you will better understand the need for strict compliance with them. The security infraction program emphasizes the importance DOE places on individual responsibilities for protecting classified information and material. I previously described a security infraction as the failure to comply with established security regulations. A person charged with an infraction could receive some type of discipline, such as a written or oral reprimand, loss of pay, or possibly even dismissal.

To ensure that you understand the significant security aspects of your job, your supervisor should hold a job level orientation with you. He should identify the classified information related to your assignment and keep you informed of your responsibilities and the security procedures to be followed. This is, of course, a two-way street between you and your supervisor. He must keep you informed, but you must ask questions any time you are in doubt or do not understand your security responsibilities.

Components of Our Security Program and Their Relationship

To provide an in-depth security system, we rely on a program composed of several elements, including personnel security, visitor control, physical security, technical security, and information security, all of which are closely interrelated.

As part of our contract with Mound, we agreed in writing not to allow any individual access to classified data until an investigation is conducted and a report made to the DOE on the character, associations, and loyalty of the individual. Based on the investigation, DOE grants two types of access authorizations, usually referred to as "Q" and "L" clearances.

The "L" clearance permits access to information up through the level of Confidential. It is based on certain national agency checks, such as the files of the FBI, CIA, and the House Committee on Un-American Activities. The other type of access authorization, the "Q" clearance, allows access to information up to and including Secret. It is based on the national agency check, plus an extensive background investigation made by the U.S. Office of Personnel Management and, in some cases, the FBI. You are subject to reinvestigation at least every five years.

Frequently, in the normal course of business, we have visitors to the site; some are cleared, whereas others are uncleared. Most are civilians, others are from the Department of Defense, and some are citizens of other countries. Visits are permitted on a "definite need" basis only. Even proposed visits by properly cleared personnel on official business must first be approved by an appropriate management official. Uncleared visitors, foreign nationals, and visitors possessing limited access authorizations (L clearances) must be escorted at all times inside the security areas. Written approval must be granted by DOE for visits by foreign nationals. Even if the foreign national is Q-cleared, his access to Restricted Data or other classified defense information is limited to only that specifically authorized by DOE.

As I previously explained, we use many physical security barriers here to safeguard classified matter. Of course, the primary purpose of physical security is to protect classified documents and material. Documents consist of any recorded information. It can be handwritten or typed. It can be a film, a rough draft, a tape recording, or a photograph. As long as it is recorded information, it constitutes a document. Material, on the other hand, refers to certain physical items, such as assemblies, components, tools, and gauges.

The basic rule is the same for both documents and material. Classified matter must be in the custody of a properly cleared individual, or it must be secured in an approved repository. Specific guidance must be applied, however, when determining the protection required for the different categories of classified documents and material or for the different levels of special nuclear material.

Finally, the components of our security program, when combined, provide for information security. Let me emphasize again that access to classified information is granted only to authorized and properly cleared persons, and then only if the information is required to perform official duties; i.e., the "need-to-know" principle.

I previously pointed out the need to comply with established security procedures and federal laws applicable to all of us. I also defined the terms "security infraction" and "security violation." An infraction is the failure to comply with established DOE security regulations. Examples include leaving a safe open and unattended, leaving a document unattended, or improperly escorting an uncleared visitor. A violation is much more serious. It involves criminal violation of federal laws covering such things as sabotage, espionage, treason, malicious mischief, and other subversive activities. Violations are investigated solely by the FBI, and a person convicted of a violation could receive fines, imprisonment, or possibly the death penalty.

It is important that you know the difference between infractions and violations. Infractions are usually committed as the result of carelessness or negligence. Violations are usually committed intentionally.

Keystone of the Security System

It should be obvious by now that DOE has gone to considerable lengths to establish physical security barriers at this plant to deny access to unauthorized persons. However, if just one employee becomes remiss in his responsibility to protect the classified information he possesses, then much of the time, effort, and money spent on our security program will have been wasted. In the final analysis, the security of this facility depends largely upon the alert, well-informed employee who conscientiously implements security regulations at all times.

Threats to Security

All countries have collection services to gather information on political, social, economic, scientific, and military developments and intentions of other countries. Such information has an important bearing on a nation's decisions, plans, and actions in international affairs and its own security. Hence, many countries spend much time, money, and effort to learn all they can of their competitors' capabilities, plans, and intentions. Many foreign countries have active intelligence services in the U.S. These include hostile services aided and abetted by countries that are their political and ideological allies. The goal of an agent from a hostile service is to obtain highly classified U.S. scientific and technical information, and the United States DOE program is a prime target. Active intelligence services include those of the U.S.S.R., Communist China, Cuba, and some European countries.

A great deal is known of how foreign intelligence operates. In some instances, a "legal" operator is posted legally in the country. He operates as an accredited diplomatic, commercial, scientific, or military officer of his country and is attached to his country's embassy or other official agency.

An "illegal" operator may be a citizen of his country working for its intelligence service or a national of a third country who operates under false identity. Supported by forged identification documents, he almost invariably lives in the target country and operates clandestinely. He has no overt association with official establishments of his country or the intelligence service for which he operates. There have been cases where apparently innocent, off-the-job contacts have been the basis for disclosures of classified information to unauthorized persons. Therefore, be alert to the possibility that, by chance or design, you could be a target of persons seeking illegal access to classified information.

Let me caution you again about the widespread use of bugging devices to obtain information. In recent years surreptitious listening devices have been vastly improved, have been miniaturized, and are produced in ingenious shapes. Examples include a microphone in a tie tack or a cuff link or a self-activating radio transmitter hidden in furniture capable of relaying conversation to a recorder miles away. Clever, efficient listening devices can be bought cheaply and freely and are easy to install in telephones, walls, equipment, pictures, etc. Remember, of course, that it is a violation of federal law to

use a surreptitious device to obtain information without the consent of the parties involved. The presence or installation of such a device is prohibited at DOE facilities. However, if you discover something you suspect is a surreptitious listening device, notify our plant security officer immediately. Do not leave the device unattended or permit it to be moved, altered, or tampered with until the security officer arrives. In addition, do not allow classified information to be discussed in the vicinity of the suspected listening device, do not indicate in the vicinity of the suspected listening device that it has been discovered, and limit knowledge of a suspected listening device to the absolute minimum number of people.

By this time you should have no doubt about the responsibilities of the individual employee and the vital role he plays in our security program. Your responsibility for protecting classified information goes with you away from the plant also. Always be circumspect in making reference to classified information. There have been cases where apparently innocent, off-the-job contacts have lead to disclosures of classified information to unauthorized persons. Be alert to the possibility that you could be the target of persons seeking illegal access to classified information. DOE offers a good question for evaluating discussions: "Could any unauthorized person possibly learn anything from such discussions that could lead to a compromise of classified information?"

Be alert at all times for circumstances that could lead to a compromise of our security interests. We all share the responsibility for promptly reporting any and all such circumstances to our supervisors or directly to the security officer.

Additional topics or explanations that may be unique to a given facility may be covered as appropriate. As a minimum, the following subjects, previously discussed with the employee during the initial security orientation briefing, should be included:

1. *Security areas of the facility.*

2. *Areas to which the employee will have access.*

3. *Use of the employee's badge (if applicable).*

4. *Articles prohibited in the facility; i.e., cameras, alcohol and alcoholic beverages, illegal drugs, copying or reproduction devices, recording devices, radio transmitters, firearms, explosives, incendiary devices, and other articles that may be used to record, transmit, or reproduce classified information surreptitiously or to cause property damage or injury.*

5. *Other local restrictions.*

6. *Current espionage cases.*

7. *Activities of hostile organizations.*

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse)

10. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *Section 783(b), Title 50, United States Code, the Intelligence Identities Protection Act of 1982, Executive Order 12356 or its successor, and Section 2003.20, Title 32, Code of Federal Regulations, so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

EXHIBIT 4

DOE F 5631.34
(10-86)
Replaces DP-354
(Previous Editions Cannot Be Used)

U.S. DEPARTMENT OF ENERGY

DATA REPORT ON SPOUSE

OMB Control No.
1910-1800

This report is required to obtain benefit under the Atomic Energy Act of 1954, as amended, and Executive Order 10450 and 10865.
PLEASE READ THE INSTRUCTIONS ON THE BACK BEFORE COMPLETING THIS REPORT.

1. Name of Employee or Applicant *(Last, First, Middle)*	2. Other Names Used by Employee or Applicant *(Maiden name and/or other names previously used)*
3. Employment *(Present assignment)*	4. Date and Place (City, State) of Marriage
5. Present Name of Spouse *(Last, First, Middle)*	6. Other Names Used by Spouse *(Maiden name and/or all other names previously used)*
7. Date and Place (City, State) of Birth of Spouse	8. Present Employment of Spouse *(Name and location)* or Last Previous Employment
9. Present Mailing Address of Spouse	10. Last Previous Address of Spouse

11. Citizenship of Spouse:
(a) ☐ U.S. . . . *Answer 12* (b) ☐ Alien . . . *Skip to 13(a)* (c) ☐ Dual Citizen . . . *Skip to 13(d)*

12. If U.S. Citizen, Indicate:
(a) ☐ By Birth . . . *Skip to 14*
(b) ☐ Derivative . . . *Answer (e) thru (g) below, then skip to 14*
(c) ☐ By Naturalization . . . *Answer (d) thru (g) below, then skip to 14*

(d) Petition No.	(f) Certificate No.
(e) Date	(g) Place (City , State)

13. If Alien, Indicate:

(a) Alien Registration No.	(d) Present Citizenship *If dual or multiple, list all countries, if U.S. is included, also complete item 12)*
(b) Date (Mo, Da, Yr) of Entry	
(c) Port (City, State) of Entry	

14. Military Service of Spouse

Country	Serial Nos.	Branch	From (Yr.)	To (Yr.)

15. Spouse's Relatives *(Parents, divorced spouse or spouses, children, brothers, sisters, stepbrothers, stepsisters, half brothers, half sisters, living or dead)*

Relation *(a)*	Name in Full *(b)*	Date of Birth (Mo, Da, Yr) *(c)*	Address *(d)*	Country of Birth *(e)*	Present Citizenship *(f)*

16. Signature of Employee or Applicant	Date	DOE File No. (To be filled in by Security Office)

EXHIBIT 5

DOE F 5631.29
(3-84)
(Previously DP-136)

OMB Approval No.
1910-1800

(Facility or Installation Where Terminated)

U.S. DEPARTMENT OF ENERGY

SECURITY TERMINATION STATEMENT

NAME AND TITLE (Print all blocks)	EMPLOYER YOU ARE LEAVING
FUTURE RESIDENCE	NAME AND ADDRESS OF FUTURE EMPLOYER:
REASON FOR TERMINATION:	
SOCIAL SECURITY NUMBER:	DATE OF BIRTH:
DATE OF TERMINATION:	DOE NUMBER (IF KNOWN)

I make the following statement in connection with the forthcoming termination of my security clearance or access authorization granted by the Department of Energy:

1. I have destroyed in accordance with DOE security regulations or transferred to persons designated by the Department of Energy all classified documents and material which I was charged or which I had in my posession.

2. I shall not reveal to any person any Restricted Data, Formerly Restricted Data, or other classified information of which I have gained knowledge except as authorized by law, regulations of the Department of Energy, or in writing by officials of the Department of Energy empowered to grant permission for such disclosure.

3. I am aware that the Atomic Energy Act of 1954 and U.S. Code, Title 18 "Crimes and Criminal Procedures," prescribe penalties for unauthorized disclosure of Restricted Data, Formerly Restricted Data, and other information relating to the national defense.

4. I am aware that I may be subject to criminal penalties if I have made any statement of material facts knowing that such statement is false or if I willfully conceal any material fact (Title 18, U.S. Code, Section 1001).

5. I know that the Department of Energy desires to be informed when former DOE or DOE contractor personnel enter the military service if they have had access to Top Secret information or classified information currently of material sensitivity to the national security.

6. I understand that the Department of Energy desires to be informed when persons who have been granted DOE access authorization propose to travel to communist countries. This does not apply to individuals who obtain DOE access authorization and receive access to Restricted Data or Formerly Restricted Data solely as employees of other Government agencies or their contractors.

(Normally, an individual will not be asked to forego any travel unless the travel is of such a nature as to be considered unwise from the standpoint of personal safety or there are special circumstances existing which would make such travel unwise from the standpoint of the national security. The DOE's security interest in such travel normally diminishes as the period of access to Restricted Data, Formerly Restricted Data or other classified information becomes more remote.)

(Signature of Person Conducting Interview)	*(Signature of Person Whose Access Authorization is Being Terminated*
(Title of Position)	*(Date)*

See reverse for Privacy Act Statement

PRIVACY ACT STATEMENT

Collection of the information requested is authorized by the Atomic Energy Act of 1954, as amended, and by Executive Orders 10865, 10450, and 12356.

The name of the individual, Social Security Number, and date of birth are used as identifying factors to establish and maintain records of DOE personnel clearance actions in the DOE System of Records DOE-42, "The Personnel Security Clearance Index." This form will become part of the individual's Personnel Security File (Department of Energy System of Records DOE-43, "Personnel Security Files").

Disclosure of the information on this form is voluntary. Access to the completed form is limited to authorized investigators from Federal agencies.

EXHIBIT 6

DOE F 5631.20
(3-83)
(Formerly DP-277)

U.S. DEPARTMENT OF ENERGY

REQUEST FOR VISIT OR ACCESS APPROVAL

(Not to be used for temporary or permanent personnel assignments.)

OMB Approval
No. 1910-1800

PART "A"

To:

From:

Date:

Prepared by:

Symbol:

Telephone No.—Commercial:

FTS:

It is requested that the following person(s) be granted visit/access approval:

LAST NAME, FIRST, MIDDLE INITIAL AND SOCIAL SECURITY NUMBER	CHECK: U.S. CITIZEN	CHECK: ALIEN	DATE OF BIRTH	ORGANIZATION	TYPE CLEARANCE	CLEARANCE NO.	DATE OF CLEARANCE

NAME OF FACILITY(IES) TO BE VISITED:	FOR THE INCLUSIVE DATES	DOE Security Official Verifying DOE Clearance

FOR THE PURPOSE OF:

TO CONFER WITH THE FOLLOWING PERSON(S):

SPECIFIC INFORMATION TO WHICH ACCESS IS REQUESTED:	Access requested to:
	Restricted Data ☐ Yes ☐ No
	Other classified info ☐ Yes ☐ No

Prior arrangements have/have not been made as follows:

CERTIFICATION FOR PERSONNEL HAVING DOD CLEARANCE

This certifies that the person(s) named above needs this access in the performance of duty and that permitting the above access will not endanger the common defense and security.

Authorized access to Critical Nuclear Weapon Design Information (CNWDI) in Accordance with DOD Directive 5210.2 ☐ Yes ☐ No

Name and Title, Requesting DOD Official

Title, Authorizing DOD Official
(See DOD Directive 5210.2 and 5210.8)

Signature
(See AR 380-150; OPNAV 5510.3F; AFR 2105-1)

CERTIFICATION FOR PERSONNEL HAVING DOE CLEARANCE

This certifies that the person(s) named above needs this access in the performance of duty.

Title

Requesting DOE or Other Government Agencies

PART "B"

Approval is granted with limitations indicated below:

Manager of Operations/or Headquarters Division Director

SEE REVERSE OF PART 5 FOR PRIVACY ACT INFORMATION STATEMENT

INDEX

	Page
Classified Document Control	7
Classified Mailing Address	16
Clearance Terminations	11
Derogatory Information	14
Mental Illness	14
Objectives	3
Personnel Identification System	4
Personnel Security Clearances	13
Physical Barriers	4
Responsibilities	3
Security Education	10
Security Infractions	11
Shipment Security	16
Storing Classified Matter	8
Surreptitious Listening Devices	17
Travel to Communist-Controlled or Sensitive Countries	16
Unaccounted for Classified Documents	7
Violations	9
Visitor Control	15

Distribution

External

TIC (2)
R. H. Caldwell, Los Alamos Technical Associates, Albuquerque, New Mexico
R. J. Eisenhauer, Universal Tool Co., Dayton, Ohio
M. W. Farmer, Gem City Engineering Co., Dayton, Ohio
A. Hansen, H&R Technical Associates, Inc., Oak Ridge, Tennessee
V. Marrow, Lockwood Greene Engineers, Inc., Oak Ridge, Tennessee
T. Morford, Mason & Hanger, Lexington, Kentucky
J. A. Morley, DOE/DAO
S. Puckett, Speedring, Inc., Cullman, Alabama
K. Schurawel, Reynolds Industries Systems, Inc., San Ramon, California
J. E. Sloane, EDO Corporation, Fullerton, California
F. R. South, DOE/DAO
L. D. Tilton, DOE/DAO

Internal

R. C. Adams (10)
D. L. Baker
J. L. Clark
C. J. Gable
K. N. Gardner (3)
M. A. Gibson (3)
V. C. Hanson
C. W. Huntington (2)
R. K. Krasnonski (2)
D. L. O'Brien
M. P. Shade
C. W. Taylor (3)
Publications
Library (15)

Lisa R. Kramer, Editor
Technical Publications