

ANNUAL REFRESHER BRIEFING

Sample Refresher Briefing for Off-Site Personnel

Department of Energy/National Nuclear Security Administration (DOE/NNSA) employees and contractors who have access authorizations (clearances) are required to complete an annual Refresher Briefing (Federal regulation 32 CFR 2001.70(e) and DOE M 470.4-1, Section K). The briefing must “selectively reinforce the information provided in the comprehensive briefing” (see first five topics in Table of Contents). If protection of special nuclear material (SNM) is part of the Comprehensive Briefing that is given at the time a clearance is granted, a refresher on SNM must be added. The briefing may also include new information or a refresher on topics covered by the Initial Briefing.

The last four topics provide additional material that might be included in a Refresher Briefing that is given to off-site personnel. These topics should be updated from year to year to highlight security requirements that are new or are the subject of recurring security incidents, or simply to keep the briefing fresh.

Refresher Briefing

Table of Contents

Purpose

Identifying Classified Information

- Classification Levels
- Classification Categories
- Declassification and Downgrading

Protecting Classified Information

- Creating and Marking
- Allowing Access
- Need-to-Know
- Discussion
- Transmittals
- Hand-Carrying
- Accountability
- Storage
- Destruction

Unclassified Controlled Information (UCI)

- Official Use Only (OUO)
- Unclassified Controlled Nuclear Information (UCNI)
- Other UCI

Reporting Foreign Intelligence/Terrorist Activity

- Reporting Requirements
- Response
- Hotline Numbers

Personal Reporting Requirements

- Access Authorization (Clearance) Reporting Requirements
- General Security Reporting Requirements
- Specific Security Reporting Requirements
- Counterintelligence Reporting Requirements

Security Outprocessing Requirements

- Property Return
- Classified Storage and Computer Access
- Termination Briefing and Statement

Operations Security

- The Threat
- What to Protect
- Countermeasures

Technical Surveillance Countermeasures

- The Threat
- Response

Prohibited and Controlled Items

- Prohibited Items
- Controlled Items

Conclusion

Purpose

DOE/NNSA employees and contractor personnel with DOE access authorizations must complete an annual Refresher Briefing to remind them of their continued responsibilities for security. Failure to complete this required briefing will result in action by the responsible DOE/NNSA office.

This briefing is designed primarily for personnel who do not regularly (if at all) conduct work at a specific DOE/NNSA site; rather, personnel perform work in areas/offices off-site. The briefing includes information on the following:

- Identification and protection of classified and unclassified controlled information (UCI)
- Requirements to report counterintelligence and security concerns
- Requirements for security outprocessing
- Operations Security (OPSEC)
- Technical Surveillance Countermeasures (TSCM)
- Prohibited and controlled items

Please complete and return your verification of briefing completion as soon as possible to _____.

Your comments and any ideas for improving this briefing are always welcome. Submit comments to _____.

Identifying Classified Information

If you are working in or supporting a classified program, your site or facility's Security or Classification Office will provide guidance in identifying what information is classified. You should work with your sponsors and supporting DOE/NNSA office to understand how that guidance applies to what you do and what you publish. You must be in a Security Area (designated for classified) when working with this information.

Most classified matter that you handle is already marked, but it is your responsibility to know when unmarked information you come across or information that you create should be reviewed for classification. If you have a question about whether something is classified, your site/facility will provide an authorized classifier who will review your document. This includes e-mails. Failure to have electronic documents reviewed for classification before distribution, including placing on the Internet or a Web site, is one of the most common security infractions.

Security requirements also apply to any discussion that involves a classified subject. It is your responsibility to tell the recipient(s) that the information being discussed is classified. You must also give its classification level (e.g., Secret) and category (e.g., Restricted Data). If you are the recipient of verbal information that you identify as classified and the security requirements have not been met, you must stop the discussion until the classification and security issues are resolved.

See next section of this briefing: Protecting Classified Information.

Classification Levels

At the time of classification, an authorized classifier will assign a classification level that indicates how sensitive the information is and the degree of damage to national security if the document were to be compromised. The three levels of classification are:

1. Top Secret (TS) – exceptionally grave damage to the national security if compromised
2. Secret (S) – serious damage to the national security if compromised
3. Confidential (C) – damage to the national security if compromised

Classification Categories

In addition to a classification level, the classifier will assign a category in accordance with subject matter. The three categories are:

1. National Security Information (NSI) – concerns national security issues
2. Restricted Data (RD) – concerns information dealing with nuclear weapon design
3. Formerly Restricted Data (FRD) – concerns military use of nuclear weapons

NSI

Presidential Executive Order (E.O.) 12958, as amended, identifies eight types of non-nuclear information classified as NSI because of national security considerations, as follows:

- Military plans, weapons systems, or operations;
- Foreign government information;
- Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- Foreign relations or activities of the United States, including confidential sources;
- Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
- U.S. Government programs for safeguarding nuclear materials or facilities;
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; and
- Weapons of mass destruction.

RD/FRD

The Atomic Energy Act (AEA) of 1954, as amended, requires information relating to nuclear energy and its use in weapons to be classified as either Restricted Data or Formerly Restricted Data, as follows:

- Restricted Data
 - The design, manufacture, or utilization of nuclear weapons
 - The production of special nuclear material (SNM)
 - The use of SNM in the production of energy

- Formerly Restricted Data
 - Primarily information that relates to the military utilization of nuclear weapons and that has been removed from the RD category by joint DOE/DoD determination

Declassification and Downgrading

If you believe a document should be declassified (you cannot identify any classified information in it) or downgraded (you identify the information as belonging in a lower classification level or category), or if you otherwise want to challenge a classification, you should contact your Security or Classification Office and talk with a derivative declassifier (DD). If declassification or downgrading appears to be warranted, a review will be conducted by the declassifier. (If your organization does not have a DD, contact an original or derivative classifier for an initial feasibility review.) The procedures for challenging the classification status of a document are simple. Your supporting Security or Classification Office will work with you and, if necessary, file your appeal through the appropriate DOE/NNSA office. Your primary contact for declassification is _____.

Protecting Classified Information

You, the individual, are the most important element in the protection of classified matter. Virtually any action you take with classified information is governed by DOE requirements and local procedures. These requirements include the generation and marking of working papers, releasing information in person or by transmittal, holding a classified discussion, or securing matter that is not in use.

Creating and Marking

All classified matter regardless of its date, office of origin, or status (draft or final) must be marked in accordance with DOE M 470.4-4-Chg 1, Ch II, 3. (Marking).

Working Papers or Drafts

If you are drafting a document on a classified topic, mark it as a working paper or draft (see DOE M 470.4-4,II,3.s). Working papers and drafts are considered as interim toward the production of a final document. The working paper does not have to be reviewed by a classifier unless it is to be released outside the office, retained more than 180 days, or filed permanently. In those cases it must be treated as any other classified document and marked appropriately.

Mark hard copies with:

- Date created.
- The highest potential overall classification level at the top and bottom of the cover page (if any), on the title page (if any), on the first page of text, and on the outside back cover or last page. In addition, mark each interior page top and bottom with the highest classification level of that page (including Unclassified) or with the overall classification level.
- The overall category (e.g., RD) at the top and bottom on the cover page (if any), on the title page (if any), and on the first page of text.

Note: The outside back cover and interior pages do not need to be marked with the category. Also, an NSI category marking is not required.

- The annotation “Working Paper” or “Draft” on first page of text.
- Applicable caveats or special markings (e.g., NOFORN) on the cover page (if any), on the title page (if any) and on first page of text.

E-Mail

For guidance on creating and marking electronic copies, see DOE M 470.4-4,II,p.(3) (Classified Electronic Mail Messages). Your site/facility's Security or Classification Office will provide local procedures.

Allowing Access

The following conditions must be met before allowing others to hear, see or use classified information:

- The individual has a valid access authorization.
- The access authorization (Q or L) is of the appropriate type for the information to be accessed.
- The individual has a "need-to-know" the information.
- The individual(s) is in an area approved for that classified activity (e.g., discussion, storage).

Need-to-Know

Need-to-know is one of the fundamental principles for the protection and control of classified information. Need-to-know is defined as:

A determination made by an authorized holder of classified or unclassified controlled information that a prospective recipient requires access to specific classified or unclassified controlled information in order to perform or assist in a lawful and authorized Governmental function.

Discussion

If you are involved in a classified discussion, it is important that only the cleared persons you have verified can hear the discussion. It is your responsibility to keep the conversation at a volume that cannot be overheard by unauthorized persons. If the conversation is not face-to-face, it must take place over an encrypted or secured telephone system.

Transmittals

If you are transmitting a classified document, you must address it to the classified address of the cleared person who will receive the document. Verify the address and

ensure all requirements for classified transmittals are followed. See DOE M 470.4-4,II,6.a.-i. (Receiving and Transmitting Classified Matter).

Hand-Carrying

If you are hand-carrying a classified document, you must comply with requirements in DOE M 470.4-4,II,6.j for hand-carrying and with any local procedures. Your site/facility's Security Office can provide guidance. It is your responsibility to verify that all requirements and procedures have been addressed before you hand-carry the matter.

Accountability

When certain classified matter is created or received, it must be entered into an accountability system and remain within the system until the matter is transferred or destroyed. See DOE M 470.4-4,II,4. (Control Systems and Accountability). Top Secret matter in any form is accountable. Secret/RD on removable electronic media is accountable and is referred to as accountable classified removable electronic media or ACREM. Secret matter that is stored outside certain types of Security Areas is accountable. Your site or facility's Information Security manager can provide details on what is accountable.

Classified documents or material may be subject to accountability because of national, international, or programmatic requirements. Accountability procedures must be strictly followed each time the classified matter is handled, and any copies that are made must be brought into the accountability system.

Storage

When classified matter is not in use, it must be properly secured. Unless a vault or vault-type room (VTR) has been approved for the open storage of classified matter, the documents or material must be stored in a GSA-approved container in a Security Area. A Security Area must have a check system that is documented in local security implementation plans. Your local Security Office can provide guidance on storage requirements that apply to containers, vaults, or VTRs. For ACREM requirements, see DOE M 470.4-4,I,8.a.(2),(a),(b),(c) (Storage-Containers).

Destruction

Classified holdings must be kept to the minimum necessary. This means that destruction of classified matter is an on-going process, which may involve extra copies, obsolete matter, or waste. You should be alert for classified matter to be

destroyed and know the correct procedures for destruction. You must use a destruction means that is locally authorized. Destruction of accountable classified requires a witness and maintenance of a record of destruction. See DOE M 470.4-4,II,8. (Destruction).

For additional information on protection requirements for classified information, you should contact _____.

Unclassified Controlled Information (UCI)

Some information that is not classified may still require protection, and it is your responsibility to identify unclassified, but controlled information, or UCI. An access authorization (security clearance) is not required. However, you must handle UCI in accordance with prescribed guidance. The UCI is kept under a locked condition when not in use.

There are several types of UCI. Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI) are the most common.

Official Use Only

Information the DOE designates as OUO is unclassified information that may be exempt from public release under the Freedom of Information Act (FOIA). This information has the potential to damage Governmental, commercial, or private interests if given to persons who do not need it to do their jobs or other DOE/NNSA authorized activities. Applicable DOE directives are: DOE O 471.3, *Identifying and Protecting Official Use Only Information*, and the accompanying Manual, DOE M 471.3-1, and Guide, DOE G 471.3-1.

The directives give guidance on identifying information that may be exempt under the FOIA. There are eight FOIA exemptions. If you determine information that you are creating or handling is OUO, you have responsibility for marking (and protecting) the information.

Page Markings

The front page of an OUO document must designate the information as Official Use Only. A prescribed front marking is applied at bottom on page (see DOE M 471.3-1,I,3. (Marking a Document that Contains OUO Information). In addition, the words, "Official Use Only" or "OUO," if more convenient, are placed at the bottom of each page that contains OUO. No top page marking is required, although some sites/facilities will mark at the top and bottom. Check your site's marking procedures for OUO.

E-mail and Other Transmittals

The first line of an e-mail message with OUO information must contain the abbreviation "OUO" before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate the attachment is OUO, e.g., "Document transmitted contains OUO information." The attachment must have all required OUO markings.

For guidance on OOU transmissions, see DOE M 471.3-1 (Contractor Requirements Document), Attachment 1.

Unclassified Controlled Nuclear Information

UCNI is defined as unclassified Government information applicable to nuclear material, weapons, and components whose unauthorized dissemination is prohibited under Section 148 of the Atomic Energy Act, as amended. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, and accompanying Manual, DOE M 471.1-1 establish the requirements. If you work with UCNI, your Security or Classification Office will provide a Reviewing Official for guidance in marking and handling.

Security measures taken to protect UCNI transmissions must deter access by unauthorized individuals and restrict public release. UCNI must be protected by an approved encryption method when transmitted over public switched broadcast communications paths such as the Internet.

Other UCI

Other types of UCI include Export Controlled Information (ECI), Naval Nuclear Propulsion Information (NNPI), Applied Technology (AT), Confidential Foreign Government Information – Modified Handling Required (CFG/MOD), and Reactor Safety Information (RSI).

For more information about UCI that you may encounter in your workplace and protection requirements, you should contact _____.

Reporting Foreign Intelligence/Terrorist Activity

Reporting Requirements

Be aware of any effort by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise you or another cleared employee. Report the following to your site/facility's Counterintelligence Office:

- All contacts by you or any other cleared employee with known or suspected intelligence officers from any country
- Any contact which suggests that you or any other employee may be the target of the intelligence service of another country or other clandestine group
- Any other known, suspected, attempted, or planned activity that threatens national security
 - A threat to national security includes: unauthorized release of or access to any classified or otherwise sensitive information; intrusion into an automated information system containing such information; or acquisition of other non-public information relating to terrorism, sabotage, subversion, or illegal diversion of U.S. technology to a foreign country.
- Knowledge of any activity by a foreign country or organization that suggests that country or organization may have unauthorized knowledge of U.S. classified information, processes, or capabilities

Response

If you become aware of any intelligence or terrorist activity against the United States, do not conduct your own investigation, put yourself in any dangerous situation, or tell family/friends of the incident. Rather, you should as soon as possible write down as many details as you can remember and report the incident to your supporting DOE/NNSA counterintelligence office or the FBI. Or call any one of the hotline numbers listed below.

If you are the target of the activity, you should not divulge any information and should not take or sign anything. You should listen carefully, be observant, and remember as many details as possible. Keep all options open by neither agreeing nor refusing to cooperate. Remain calm, be noncommittal, ask for time, and report immediately to your counterintelligence office.

Hotline Numbers

Some Federal agencies maintain hotlines to provide an unconstrained avenue for Federal and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities, fraud, or other infractions.

Federal and contractor personnel are encouraged to furnish information through established DOE/NNSA or company channels. However, the hotline may be used as an alternate means to report this type of information when you consider it prudent or necessary to do so. The following are relevant hotline telephone numbers.

DOE/NNSA

Office of Counterintelligence (CI)202-586-1247
Inspector General1-800-541-1625
(for criminal violations such as fraud related to DOE/NNSA programs)

Federal Bureau of Investigation (FBI)

The FBI has 56 field offices. The phone number of the nearest office is listed under U.S. Government in your local phone book and it is: _____.

Department of Defense (DoD):1-800-424-9098, 703-693-5080

Department of Army.....1-800-CALLSPY

Air Force Office of Special Investigations202-767-5199

Naval Criminal investigative Service.....1-800-543-NAVY

Defense Security Service (DSS)

(Defense contractors report suspected incidents to local DSS industrial security representative)

Defense Intelligence Agency (DIA)703-907-1307

National Security Agency (NSI)301-688-6911

Central Intelligence Agency (CIA)

Office of the Inspector General.....703-874-2600

Department of State

Bureau of Diplomatic Security202-663-0739

Note: When traveling overseas, report suspected incidents to the Regional Security Officer (RSO) or Post Security Officer (PSO) at the nearest U.S. diplomatic facility.

Nuclear Regulatory Commission (NRC)

Office of the Inspector General.....1-800-233-3497

Customs Service.....1-800-231-5378
(to report suspicious activities involving export of high-technology, munitions products, other commodities, narcotics, intellectual property, and U.S. currency)

Department of Commerce/
Office of Export Enforcement202-482-1208 or 1-800-424-2980
(to report suspicious targeting of U.S. export-controlled commodities)

Personal Reporting Requirements

Access Authorization (Clearance) Reporting Requirements

As a condition of holding a DOE access authorization, you are required to undergo a reinvestigation to maintain it. Reinvestigations are conducted as follows:

- Every five years if you have a Q access authorization
- Every ten years if you have an L access authorization

At that time, you will be given 30 days to complete a new or updated Questionnaire for National Security Positions (QNSP), but it is to your advantage to report serious security concerns as they arise rather than wait to report them on the QNSP. Report security concerns, such as a traffic violation that is alcohol or drug-related, to your site/facility Security Office. You may be investigated sooner whether you have reported them or not.

General Security Reporting Requirements

All DOE/NNSA and contractor personnel, whether cleared or uncleared, are required to report when their badge is lost, stolen, or misused. You must also report incidents of safeguards and security concern to your Security Office. This is especially important when you become aware that classified matter has been or may have been lost or compromised. Waste, fraud and abuse, whether a crime is involved or not, must be reported to the Inspector General.

Specific Security Reporting Requirements

Some security concerns must be reported as they occur. You must immediately report:

- Approaches or contacts by anyone seeking unauthorized access to classified information or matter or to special nuclear material.
- Violations of security regulations.

Cleared employees and contractors must notify their site/facility's Personnel Security Office verbally within two working days followed by written confirmation within the next three working days of the following:

- All arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of law within or outside of the United States
 - Traffic violations for which a fine of up to \$250 was imposed need not be reported unless the violation was alcohol or drug related.
- Personal or business-related filing for bankruptcy
- Garnishment of wages
- Legal action effected for a name change
- Change in citizenship
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national
- Hospitalization for a mental illness; treatment for drug abuse; or treatment for alcohol abuse

Cleared employees and contractors must complete DOE F 5631.34, "Data Report on Spouse/Cohabitant," within 45 working days after a marriage or cohabitation begins. Your Personnel Security Office can provide you with a form.

Counterintelligence Reporting Requirements

In addition to the required reports discussed in "Reporting Foreign Intelligence/Terrorist Activities," DOE/NNSA and contractor personnel, whether cleared or uncleared, must report the following to their supporting DOE/NNSA Counterintelligence Office:

- Deliberate compromise or foreign involvement in suspected compromise of classified information
- All substantive contacts or relationships with citizens of sensitive countries
- Official travel to sensitive countries or travel to non-sensitive countries if it involves a sensitive subject (at least 45 days prior to departure date)
- Official travel to a non-sensitive country (at least 30 days prior to departure)
- All foreign travel done with substantive foreign monetary support (upon learning of such support)

- Unofficial travel to sensitive countries (at least 30 days prior to departure) if at or supporting the following laboratories: Los Alamos National Laboratory, Lawrence Livermore National Laboratory, or Sandia National Laboratories

Security Outprocessing Requirements

DOE/NNSA and many of its contractors have a continual problem implementing requirements that apply to cleared personnel who are terminating an access authorization or transferring an access authorization to other facilities. Contact your site/facility's Personnel Security Office for requirements and a procedure.

Property Return

If you are terminating employment at a site or transferring, you have responsibility to return certain property. Accountable classified matter must be returned, along with any other classified documents/material held by the individual. If you signed for any property, you must return that property before you leave. Badges must be returned on leaving a site (even if not working physically at the site). Contact your Security Office for a procedure for badge return. Every year there are departing personnel who fail to turn in their badge; many cleared individuals do not view a DOE security badge as Government property. Badges are a key component of a site's physical security. Like badges, keys are also a security component that must be returned.

Classified Storage and Computer Access

Security container or vault combinations known by terminating personnel must be changed. Before you leave a site, you should remind the appropriate custodians that you will no longer require access. You may need to take action to cancel access to certain computer networks and programs.

Termination Briefing and Statement

The terminating individual has responsibility to schedule a Termination Briefing and complete a Security Termination Statement, DOE F 5631.29. Some individuals may avoid or evade these requirements in the mistaken belief that it will keep their access authorizations active. The Termination Briefing and signed statement are required by Federal regulation.

Operations Security (OPSEC)

OPSEC is a countermeasures program designed to disrupt or defeat the ability of an adversary to exploit classified or unclassified controlled activities or information and to prevent the inadvertent release of such information. OPSEC is not a traditional security program; rather, it is a program to augment or strengthen from within other DOE/NNSA Safeguards and Security programs such as physical, information, personnel, and communications security. OPSEC supplies the common link to other security programs through employee involvement.

The OPSEC Program is designed to enforce each person's awareness and understanding of the importance of Operations Security. As the name implies, the individuals within the operation are the ones who implement the security measures used to protect sensitive information.

The Threat

The growing threat of industrial and economic espionage was once thought to come only from military adversaries; however, in recent years, the espionage threat has surfaced among political and economic allies. Economic competition from countries of the former Soviet Union and the Third World means the United States must treat virtually every nation as an economic foe.

In today's environment, targeted information does not need to be classified to be valuable. Seemingly insignificant bits and pieces of information can be gathered and analyzed. To an adversary, nothing is irrelevant; these groups consider each piece of information a part of a puzzle. If the information does not fit current needs, it is put on a shelf for future reference.

Individually, you make up one of the most accessible sources of intelligence information that adversaries will attempt to exploit, and the information you have may be dispersed in various careless and mundane ways:

- Through conversations in person, on the telephone, as a speaker at a conference, or as shop talk in unsecured areas such as restaurants, bars, airports, and other public places
- Through memos and reports that are prepared, distributed, and then disposed of as unclassified waste, or distributed to persons not having a legitimate need
- Through probing media interviews, public hearings, and Freedom of Information Act requests—all legitimate activities in a free society, but care must be taken in all responses

What to Protect

In the language of OPSEC, subjects worthy of protection are referred to as Critical Program Information (CPI) with associated indicators.

CPI is the “big picture.” In the corporate environment, the big picture is a major program about which military or economic adversaries want to gain information: long term research and development plans, a scientific breakthrough, production quantities, etc. Your supervisor is in the best position to tell you about these sensitive issues. Many organizations have a Critical Program Information List (CPIL) that you should read to become familiar with what requires protection. Another way of describing CPI is to equate it to a family vacation that will leave your home vacant. The fact that your home will be vacant, including length of time, is considered critical program information.

“Indicators” are pathways of information that would lead someone to conclude you are on vacation without having prior knowledge of that fact. For example, several newspapers lying in your driveway, an overstuffed mail box, advertising flyers sticking in your front door, or lights left on all night are signs no one is home.

So it is with company information. Out-of-the-ordinary purchase requests for specialty items, unique raw materials, even rosters listing the names and titles of company employees, can all give an adversary insight into sensitive programs. Remember, economic and military opponents will patiently spend years gathering information out of trash cans, intercepting phone conversations and faxes, or attending professional symposia in order to put the pieces of the puzzle together. If your organization has a CPIL, it will have supporting indicators so you can see how the “sum of the parts could equal the whole.”

Countermeasures

- Limit the amount of detail included in documents that go to outside vendors.
- Limit distribution of documents to only those people/agencies that absolutely need them. Do not release information outside the organization without prior approval of your supervisor or the communications office, or if the information was developed under DOE or NNSA sponsorship, compliance with the OUO directives.
- Destroy sensitive documents when no longer needed in accordance with procedures.
- Ensure that purchase requisitions and related documents do not specify an association between acquisition of unique or specialized items and a sensitive program.

- Do not discuss sensitive programs over the phone and especially avoid cellular and cordless instruments.
- Use OPSEC headers, footers, or banners on sensitive correspondence.
- Mark and protect computer disks containing unclassified controlled information and refrain from transmitting such data on the Local Area Network or via modem to other terminals.

Technical Surveillance Countermeasures

Technical surveillance countermeasures (TSCM) are those measures taken to detect, deter, and nullify espionage committed through technologies designed to obtain classified or controlled information. TSCM technicians use several techniques and a variety of electronic and electrical equipment to detect illegal devices designed to listen and/or transmit information, more commonly known as “bugs.” However, even if your area does not receive TSCM support, you should be concerned about illegal listening devices like bugs and taps, which can be and have been used for many purposes other than collecting classified information.

The Threat

The potential threat can come from foreign intelligence services, business competitors, terrorists, disgruntled business partners, friends and relatives, organized crime, and the news media. If you suspect or become aware of a technical surveillance penetration, you need to know the proper procedures for protecting the information and evidence and reporting the incident.

Response

You are responsible for responding to any indication of surveillance. Some warning signs of potential covert surveillance include sudden changes in the performance of your telephone, cell phone, or other office equipment; private or confidential business information is found in the public domain; and information discussed during a private meeting is quickly known to others without a need-to-know the information.

You should take the following actions:

- Stop all sensitive discussions and activity in the area.
- Protect the area so that no one can remove the suspected device.
- Immediately report the incident to your site/facility Security Office by the most secure means available. Any discovery of a possible technical surveillance penetration is reportable. Do not discuss details over the phone or in close proximity of the device. When you contact Security, simply state that you need to talk to a TSCM Officer immediately. The fact that a possible technical surveillance may exist is classified.
- To the extent possible, continue non-sensitive, routine activities.

- When the appropriate authorities arrive, brief them about the situation away from the suspected device.

Prohibited and Controlled Items

Certain items are not allowed into Security Areas based on Federal law or regulation, or DOE directives. These items are referred to as “Prohibited Items.” Some Government or privately owned items that are designated “Controlled Items” are also not allowed in certain Security Areas based on DOE directives and local site policy without prior authorization.

Prohibited Items

The following items are prohibited on all DOE/NNSA sites unless approved in advance by the responsible DOE/NNSA office:

- Dangerous weapons (includes firearms, ammunition, stun-guns, knives with long blades, swords, knuckles, blackjacks, tomahawks, bows and arrows, spears, switchblades, simulated weapons)
- Explosives (includes chemical dispensing, incendiary, and explosive devices)
- Instruments or material likely to produce substantial injury to persons or damage to persons or property
- Controlled substances (drugs and paraphernalia, but not prescription drugs)
- Any other items prohibited by Federal regulation

Controlled Items

Government and privately owned portable electronic devices that are capable of recording information or transmitting data are Controlled Items that are not allowed in most Security Areas unless specifically authorized. Sites may add other items to the list. At your site, the following are Controlled Items:

Conclusion

Congratulations! You have completed your DOE/NNSA Refresher Briefing. It is the responsibility of the facility holding your access authorization to properly record the completion of your briefing. You must complete any certification requirements your Security Office has forwarded to you and return documentation in accordance with instructions. If further assistance is necessary, please contact

_____.