Counterintelligence Reporting Requirements
In The Department of Energy

In the wake of highly publicized allegations of foreign espionage at DOE laboratories, and following the issuance of a Presidential Decision Directive in 1998, DOE has made sweeping changes in security and counterintelligence (CI). Organizational structure has been changed and new policies have been issued. All of these efforts have been intended to strengthen the security of sensitive information and resources under our care.

As we in the Office of Counterintelligence (OCI) have worked to develop, implement and explain the new CI reporting policy, some of the feedback we've received suggests that we have not been as effective as we had hoped, particularly with regard to the need to report certain relationships with citizens of sensitive countries. The purpose of this document is to clarify CI reporting policy by essentially "cleaning the slate" and starting anew. Our objective here is to provide a simple, but comprehensive, statement of reporting requirements, drawing essential content from prior guidance while attempting to eliminate confusion. This restatement of policy takes into consideration all prior CI reporting requirements, including the Close and Continuing Contact policy set forth in DOE Notice 142.1, "Foreign Visits and Assignments" and the foreign contact reporting required by DOE Order 551.1, "Official Foreign Travel". In instances where this new formulation may conflict with prior statements of policy, this new guidance will be followed.

Attachments:
1) CI Reporting Requirements and Glossary
2) Frequently Asked Questions
3) CI Reporting Matrix

Counterintelligence Reporting Requirements

Background

When setting out to improve understanding of ideas, concepts and policies, it is generally helpful to first define terms. The definition of Counterintelligence (CI) that we will be using comes directly from Executive Order 12333, December 4, 1981, "United States Intelligence Activities":

> Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

You may have noted something unusual about this definition; it not only describes what Counterintelligence IS, but also what it IS NOT. Counterintelligence concerns itself with "countering" the efforts of foreign "intelligence" agencies. It does not include responsibility for

personnel, physical or communications security (the latter two sometimes known as the "gates, guns and guards" types of security)

While CI and Security have separate concerns and areas of responsibility, both are essential to overall success in protecting information and resources. They complement one another. DOE, like other federal agencies, implements E.O. 12333 based on guidelines issued by the U.S. Attorney General. These guidelines provide specific rules for handling information and protecting the privacy (and other rights) of U.S. persons. The Counterintelligence Officers (CIOs) in OCI follow these guidelines and other applicable federal statutes, laws and DOE directives.

The CI measures we are taking are based on our best understanding of the current foreign intelligence threat. We assess the threat by collecting and reviewing DOE CI information, and learning from our U.S. Intelligence Community partners. What we know is that despite the end of the Cold War virtually every country has continued to maintain a foreign intelligence service, and they task those services to gather information, including sensitive and classified DOE information. Some countries are thought to pose a greater risk than others, and DOE (NN-43) has developed a "Sensitive Countries" list to identify them as warranting special attention.

A foreign intelligence service collects human intelligence (HUMINT) either through direct observation by one of its members or, if that's not feasible, from another person in a position to know. While we are concerned about either method, the latter one is what has given rise to the policy to report certain contacts or relationships with citizens of sensitive countries, or unusual requests for classified information by any persons not authorized to have it (we recognize that information is also gathered in other ways, such as by monitoring telecommunications, satellite imagery, or other technical means).

Why do we need these reporting requirements? We know that foreign intelligence services are still active, and they spend a great deal of time and effort cultivating relationships with people in "useful" positions, in the hope of being able to gather information from those individuals (perhaps only to learn that another person might be even more useful to them). As any relationship develops, its characteristics will depend on a variety of complex factors, such as the likes and dislikes, hopes, dreams, and professional goals of each of the two people in the relationship. However, in this "special" kind of relationship, the foreign intelligence officer carefully manipulates any factors s/he can control, in order to achieve the outcome s/he wishes.

The relationship may continue to be overtly cordial and professional, if the intelligence officer is successful in "eliciting" information from a targeted person. Or, it may evolve into a situation where the targeted person is "recruited" to provide information, either by blackmail or promise of reward, and understands that s/he is working for a foreign intelligence service. It is natural for individuals to discount the subtlety of these kinds of approaches, and the need to report contacts to CI officers. Most people probably feel that they are keenly aware of the potential for such ploys and very capable of detecting attempts to form relationships for ulterior motives.

The key point here is that virtually every intelligence service follows the same process for developing these relationships…..relationships that are vital to their information collection task.

Many agents of foreign intelligence services are highly skilled in establishing these seemingly innocuous relationships, and it can be helpful for the DOE person to know that they are interacting with a known or suspected intelligence officer. The process essentially involves: Spotting, Assessing, Cultivating, Recruiting, Handling, and Termination.

Spotting simply refers to the job of finding someone in a position that is "useful" to the foreign intelligence officer. This may be achieved through personal contact, or by reviewing such things as phone books, web sites, or attending scientific symposia. Once a person is identified, through whatever means, the assessment and cultivation begin. And this is where the policy to report relationships is important. It is intended to help us know if a relationship we are developing with a citizen of a sensitive country is harmless or potentially harmful. A "harmful" relationship would be one in which a foreign intelligence officer attempts or even succeeds in eliciting information, or attempts or succeeds in recruiting and then "handling" the person until the relationship is "terminated", when it is no longer useful.

Government Policy for CI Reporting

The government's policies for CI reporting are intended to counter the threat from foreign intelligence services' HUMINT (human intelligence) activities, as described above. DOE and other federal agencies implement laws and directives to address their unique needs, insuring minimum requirements are met and imposing more stringent measures where indicated. DOE's CI reporting requirements derive principally from four sources: the Atomic Energy Act of 1954, and three subsequent Presidential documents.

The Atomic Energy Act of 1954, as amended, authorizes the Secretary of Energy to protect against disclosure, information that could adversely affect the health and safety of the public or the common defense and security of the United States.

Executive Order 12333, December 4, 1981, "United States Intelligence Activities", requires the Secretary of Energy to develop and implement policies and programs, which provide for the security of U.S. Government energy operations. This includes consultation with federal agencies regarding Foreign CI issues. DOE follows U.S. Attorney General Guidelines in implementing the executive order.

Presidential Decision Directive (PDD)/NSC - 12, August 5, 1995, "Security Awareness and Reporting of Foreign Contacts," mandates that each Department or Agency of the U.S. Government maintain a formal security and/or CI awareness program which includes periodic briefings or briefings prior to foreign travel and provides for the reporting of employee contacts with foreign nationals. It directs agencies to "….tailor [their program] to meet the particular functions of the agency or department and the vulnerability of certain categories of employees who, through either job function or access to classified or sensitive information or technology, could be the target of exploitation by foreign intelligence services".

White House Memorandum, August 23, 1996, "Early Detection of Espionage and other Intelligence Activities Through the Identification and Referral of Anomalies", communicates to

federal agencies the President's guidance to report observations of unexpected activities occurring during U.S. defense and other national security operations.

These legislative and executive policies are intended to counter the foreign intelligence threat in part by insuring that employees report information that would help identify espionage activities and attempts.

DOE CI Reporting Requirements

Adhering to the President's direction (in PDD/NSC-12) to insure that our program is tailored to address the extreme sensitivity of DOE information and resources and the vulnerability of our people (many of whom are in close contact with sensitive country foreign nationals), we have opted for a fairly robust CI reporting program. At the same time, we have attempted to ensure that our reporting requirements do not intrude on the privacy of employees or their freedom of association. We have carefully built upon the basics of PDD/NSC-12 by adding a requirement that employees also report certain Professional, Personal and Financial Relationship information. These, together with the requirement to report anomalies, will help insure that DOE people, information and resources are protected from foreign intelligence efforts.

Current DOE CI reporting requirements are as follows:

Professional Relationships: DOE personnel are required to report professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad. This is often captured in trip reports or other formal, routine documentation of professional activity. It may also be gathered directly by CIO's. DOE travelers to sensitive countries must notify CIO's of their impending travel so that they may receive CI briefings and be debriefed upon their return. Likewise, visits and assignments of sensitive country foreign nationals are coordinated with OCI, as are visits of any foreign nationals who are going to be given access to sensitive subjects. Another requirement is that DOE personnel notify a CIO of any foreign travel for which foreign monetary support is provided, whether to a sensitive or non-sensitive country.

Personal Relationships: Substantive personal relationships with sensitive country foreign nationals (who are not permanent resident aliens), other than family members, also must be reported to your CIO. A substantive relationship is one that is enduring and involves substantial sharing of personal information and/or the formation of emotional bonds. An enduring relationship is one that has existed, or is expected to exist, for a substantial period of time (months or years). Substantial sharing of personal information involves discussion of "private" information about oneself (that one would not routinely share with strangers, for instance). Emotional bonds refer to feelings of affection or emotional attachment in a relationship. Because the concepts of "personal information" and "emotional bonds" are necessarily subjective, we must rely on the judgment of each individual as to the existence of, and a reporting threshold for, these criteria. Examples of relationships that in our opinion do, and do not, meet the reporting threshold are found in the appendix, to aid you in reaching conclusions regarding your particular circumstances. The personal relationship may arise through contacts at work or off-duty activities, or even in cyber-space, should a relationship form in the course of

internet or email contact. Regardless of location, all such relationships with non-family sensitive country foreign nationals are reportable.

Financial Relationships: In addition to professional and personal relationships, certain financial relationships are also reportable. Substantive business transactions citizens of sensitive countries (who are not permanent resident aliens) must be reported, whether they involve one-time interactions or on-going financial relationships. The requirement pertains to non-incidental financial transactions. Small payments for such things as house cleaning or other such personal services are not included in the requirement. Partnerships or other business interests or investments are the focus of this reporting requirement, because they provide the potential for exploitation or pressure. Financial support provided to family members is not included.

Unusual Solicitations: PDD/NSC –12 requires employees to report any attempts by unauthorized persons to gain access to classified information. The reporting requirement is not limited to sensitive country foreign nationals, or even just foreign nationals, but rather pertains to attempts by any unauthorized person, even U.S. citizens. The attempts may be in the form of pointed questions or subtle elicitation. This directive also requires employees to report situations in which they feel they may be targeted for exploitation by a foreign intelligence service (for example, if one is traveling abroad and asked to carry a sealed package back to the United States……which could lead to a customs search at the border and disclosure of illegal contraband).

Anomalies: Another consideration in CI reporting has to do with anomalies. An anomaly of interest to CI is defined as:

> ….foreign power activity or knowledge, inconsistent with the expected norm, that suggests foreign knowledge of U.S. national security information, processes or capabilities.

In 1996 the White House issued a memorandum, signed by the National Security Advisor, requiring federal employees and contractors to report anomalies that arise in the course of their day-to-day work. As explained in the memorandum, U.S. CI experience has demonstrated repeatedly that observations of unexpected activities occurring during U.S. defense and other national security operations can be indicators of foreign knowledge of these operations. For example, the Soviet Navy's seeming foreknowledge of where U.S. ships were going was much later found to be attributable to the John Walker spy ring. The sudden inability of U.S. intelligence to continue exploitation of Russian communications vulnerabilities was, much later, traced to the espionage of Ronald Pelton. Agencies aware of these events did not consult CI elements in a timely manner about their anomalous observations. Those in Intelligence Community analytical circles felt that if these "anomalies" had been reported earlier, the spying might have been discovered at a much earlier time. The DOE Office of Counterintelligence is responsible for collecting reports of such anomalies and forwarding them to the Intelligence Community.

Espionage Indicators: Just as a retrospective study of espionage cases suggested the need to be aware of CI anomalies, similar studies have indicated a need to be aware of certain problems and

behaviors of coworkers. While much of the preceding discussion has addressed thwarting the efforts of foreign intelligence services to enlist the aid of Americans it is a sad fact that most espionage cases have involved Americans who have volunteered their services. The situation in which a cleared employee decides to commit espionage and takes the initiative to establish contact with a foreign intelligence service is known as the "Insider Threat".

Recent U.S. history has many examples of the Insider Threat, such as Aldrich Ames in the CIA and Jonathan Pollard in the Defense Intelligence Agency. Studies of Ames, Pollard and others have yielded some potentially helpful information about the behaviors and personal qualities and characteristics of individuals who have engaged in espionage. While common features abound, it is important to note that the factors we have identified are "descriptive" and not "predictive". That is, certain behaviors, personal problems and personality characteristics have been found to be associated with persons who have engaged in espionage, but they by no means are exclusive to that set of people. There are many people who are confronted with similar problems and circumstances who do not engage in espionage. The lesson here is that managers and coworkers should be sensitive to these kinds of indicators, and take steps to aid those who appear to need help, and report behaviors that suggest espionage activity. Espionage indicators include:

Attempts to obtain information without need to know
Unexplained/excessive use of copiers
Living beyond one's means
Unusual foreign travel patterns
Personal Problems

Classic indicators have been evident in many recent cases of espionage when they have been examined after they have been closed. Aldrich Ames, for instance, was clearly living beyond his means, and was engaged in unusual travel. He also continued to obtain access to information for which he had no professional need. Jonathan Pollard used copy machines excessively, and was known to brag about expensive holiday trips that seemed to be lavish beyond his means.

Research conducted on espionage perpetrators shows in many instances that they were having significant problems that they felt unable to cope with (e.g. financial, relationship, work, etc.). While the vast majority of people with such problems do not resort to espionage, virtually all could have benefited by some social intervention and perhaps some might not have ended up involved in espionage activities.

We are not suggesting that we need to be overly vigilant with regard to our coworkers….we don't want to get to the point that people don't feel free to be themselves or are continually uncomfortable with the thought of being under constant scrutiny. Rather, we are simply asking that we slightly lower the threshold at which we are willing to act. All could benefit from increased alertness to indicators and a greater willingness than we may have had in the past to bring significant information to the attention of supervisors and/or CI officials.

Legal Protections

In the United States individual freedoms are protected by the Constitution. Activities designed to help insure our national security must be carefully considered and implemented to insure they do not illegally infringe on personal rights and liberties. Law enforcement and security agencies operate under carefully crafted guidelines to insure that constitutional rights are protected. The same guidelines that govern our collection of information about U.S. persons also provide an oversight function and legal sanctions for improper collection or retention of information. While a comprehensive review of employee legal rights and protections would be beyond the scope of this document, a general overview of legal considerations related to DOE OCI activities may be useful.

Within DOE, the Offices of Intelligence and Counterintelligence operate under guidelines set forth by the Attorney General of the United States pursuant to E.O. 12333. These Attorney General Guidelines are intended to enable the DOE to effectively carry out its authorized functions as a member of the U.S. Intelligence Community, and to "…..ensure that DOE intelligence activities and programs do not violate constitutional protections and other individual rights of "U.S. Persons" as defined in E.O. 12333".

While some other members of the Intelligence Community have authority for covert activities, DOE OCI does not. Any information regarding foreign energy matters collected by DOE employees in the course of their work must be collected overtly, with no attempts made to conceal the activity. Accordingly, DOE CI cannot task DOE employees to gather information regarding foreign personnel or capabilities, though information gathered incidental to their work may be shared with OCI.

OCI has authority to gather CI-relevant information concerning U.S. persons and to maintain a system of records to make use of that information. For instance, pre-briefings and debriefings of travelers and hosts are documented in the system of records. Annual reviews are conducted to insure only authorized information is retained.

When a DOE person comes to OCI with suspicions or concerns that another DOE person may be involved with or vulnerable to a foreign intelligence service, it is our policy to handle such matters discretely. We can take steps to insure that the identity of the reporting individual is protected within the CI community, while we work to gather information about the allegation. Ultimately, the anonymity of the person coming forward will depend on many factors, including the nature of the offense and the possibility of collecting information that independently confirms the suspicions. OCI insures that information regarding U.S. persons is lawfully collected and then carefully controlled and disseminated within the Intelligence Community following E.O. 12333 restrictions.

Individual Participation is Key

The CI Reporting Requirements discussed here are a key part of a comprehensive program to: 1) inform DOE employees and contractor personnel about the foreign intelligence threat and, 2) obtain their active support in countering the threat. Effective counterintelligence requires a team effort. All employees and contractor personnel must be aware of the threat and be willing to report CI-relevant information. Providing CI awareness information to the entire DOE population is a formidable challenge. Encouraging people to report CI information adds to the challenge, as we must overcome natural tendencies to rationalize or otherwise talk oneself out of becoming involved.

We also recognize that even if everyone were in agreement regarding the foreign intelligence threat, reasonable people may differ with respect to what steps are necessary to counter the threat. The CI reporting requirements described here represent our best understanding of the threat and the least intrusive means to effectively counter it. The CI program has received the endorsement of the Secretary and his senior management team. Laboratory directors and site managers are responsible for effective CI programs at their locations, and are expected to support these requirements. Likewise, contracts will be revised to insure CI concerns are addressed as performance elements.

We solicit your support and welcome constructive feedback on how together we can most effectively counter the efforts of foreign intelligence services and protect DOE personnel and resources. Please contact your servicing CIO if you have questions or wish to provide feedback.

Glossary

Administrative Investigation: An administrative investigation involves the non-intrusive gathering of facts from existing DOE records in order to confirm or refute CI allegations. An administrative investigation is not a law enforcement investigation. If an appropriate threshold of information is developed as a result of an administrative investigation, the matter will be referred to the appropriate law enforcement officials for investigation.

Assignment: Presence, including employment, of an invited foreign national at a DOE facility for more than 30 calendar days. Assignments are normally for the purpose of participating in the work of the facility, gaining experience, or contributing to projects.

Counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, communications, or documents and other matter security programs.

Espionage: Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation.

Foreign National: For CI Reporting purposes, a foreign national is any person who is not a U.S. person.

Indices Check: A national security check. Accomplished by requesting information from appropriate U.S. Government agencies to determine whether information exists on a particular foreign national.

Preliminary Inquiry: A preliminary inquiry is defined as the collection and examination of information such as records reviews and personnel interviews to assess CI concerns. Preliminary inquiries are limited in scope and duration and are conducted for the primary purpose of determining whether a basis exists to initiate an investigation.

Sensitive Countries List: Prepared by NN-43. Countries appear on this list for reasons of national security, nonproliferation, anti-terrorism, or economic security. Due to the dynamic nature of world events the list may change over time. For purposes of the CI Reporting requirements a person is considered to be from a sensitive country if a citizen of, or employed by a government or institution of, a sensitive country.

Sensitive Subjects List: Unclassified subjects/topics identified in existing Federal regulations governing export control as well as those identified by DOE as unique to its work, which involves information and/or technologies that are relevant to national security. Disclosure of sensitive subjects has the potential for enhancing weapons of mass destruction capability, leading to weapons of mass destruction proliferation, divulging militarily critical technologies, or

revealing other advanced technologies which may adversely affect U.S. national economic security. Therefore, they require special management oversight, especially prior to release to foreign nationals. The list of Sensitive Subjects is maintained by NN-43.

United States Person: For the purposes of CI Reporting guidance a U.S. person means a United States citizen, a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed or controlled by a foreign government or governments.

Visit: Presence of a foreign national at a DOE facility for 30 calendar days or less. Visits which total over 30 calendar days in a period of 12 months are defined as assignments. Visits are normally for the purpose of technical discussions, orientation, observation of projects or equipment, training, contract service work, or discussion of collaboration on topics of mutual interest without participation in the work of the facility, or for courtesy purposes. The terms "visit" includes officially-sponsored attendance at a DOE event off-site from a DOE facility, but does not include on or off-site events and activities open to the general public.