Proposed Rules

Federal Register

Vol. 70, No. 5

Friday, January 7, 2005

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF ENERGY

10 CFR Parts 709 and 710

[Docket No. CN–03–RM–01]

RIN 1992–AA33

Counterintelligence Evaluation Regulations

AGENCY: Office of Counterintelligence, Department of Energy.

ACTION: Supplemental notice of proposed rulemaking and opportunity for public comment.

SUMMARY: The Department of Energy (DOE or Department) publishes a supplemental notice of proposed rulemaking to establish new counterintelligence evaluation regulations, including revised regulations governing the use of polygraph examinations. This proposed rule substitutes for DOE's April 14, 2003, preliminary proposal to retain the existing Polygraph Examination Regulations without significant change. The statutory purpose of the regulations, as stated by section 3152 of the National Defense Authorization Act of Fiscal Year 2002, is ''* * * to minimize the potential for release or disclosure of classified data, materials, or information.'' The main features of today's supplemental proposal are: Significant reductions in the number of individuals now subject to mandatory counterintelligence evaluations including polygraph screening; initiation of random counterintelligence evaluations including polygraph screening to deter unauthorized releases or disclosures; strict prohibitions on the use of polygraph examination results as the sole basis for adverse actions against employees; and a program description showing how polygraph examinations are used as one of a broad array of tools to deal with counterintelligence risks.

DATES: Written comments (10 copies) are due March 8, 2005. You may present oral views, data, and arguments at the public hearing which will be held in Washington, DC on March 2, 2005 at 10 a.m. If you would like to speak at this hearing, contact Andi Kasarsky at (202) 586–3012. Each oral presentation is limited to 10 minutes. The hearing will last as long as there are persons requesting an opportunity to speak.

ADDRESSES: You may choose to address written comments or notification of intent to speak at the public hearing to U.S. Department of Energy, Office of Counterintelligence (CN–1), Docket No. CN–03–RM–01, 1000 Independence Avenue. SW., Washington, DC 20585. Alternatively, you may e-mail your comments or your notification to: *poly@cn.doe.gov.* You may review or copy the public comments DOE has received in Docket No. CN–03–RM–01, the public hearing transcript, and any other docket material DOE makes available at the DOE Freedom of Information Reading Room, Room 1E–190, 1000 Independence Avenue, SW., Washington, DC 20585. This notice of proposed rulemaking and supporting documentation are available on DOE's Internet home page at the following address: *http://www.so.doe.gov.* The public hearing for this rulemaking will be held at the following address: U.S. Department of Energy, room 1E–245, 1000 Independence Avenue, SW., Washington, DC. For more information concerning public participation in this rulemaking, see Section VI of this supplemental notice of proposed rulemaking.

FOR FURTHER INFORMATION CONTACT: Douglas Hinckley, U.S. Department of Energy, Office of Counterintelligence, CN–1, 1000 Independence Avenue, SW., Washington, DC 20585, (202) 586–5901; or Robert Newton, U.S. Department of Energy, Office of General Counsel, GC–53, 1000 Independence Avenue, SW., Washington, DC 20585, (202) 586–6980. For information concerning the public hearing, requests to speak at the hearing, submissions of written comments or public file information contact: Andi Kasarsky at (202) 586–3012.

SUPPLEMENTARY INFORMATION:

I. Introduction

Under section 3152(a) of the National Defense Authorization Act for Fiscal Year 2002 (NDAA for FY 2002), DOE is obligated to prescribe regulations for a new counterintelligence polygraph program the stated purpose of which is ''* * * to minimize the potential for release or disclosure of classified data, materials, or information'' (42 U.S.C. 7383h–1(a).) Section 3152(b) requires DOE to ''* * * take into account the results of the Polygraph Review,'' which is defined by section 3152 (e) to mean ''* * * the review of the Committee to Review the Scientific Evidence on the Polygraph of the National Academy of Sciences'' (42 U.S.C. 7383h–1(b), (e)).

Upon promulgation of final regulations under section 3152, and ''effective 30 days after the Secretary submits to the congressional defense committees the Secretary's certification that the final rule * * * has been fully implemented, * * *'' section 3154 of the National Defense Authorization Act for Fiscal Year 2000 (NDAA for FY 2000) (42 U.S.C. 7383h), would be repealed by operation of law. (42 U.S.C. 7383h–1(c).) The repeal of section 3154 would eliminate the existing authority which underlies DOE's current counterintelligence polygraph regulations, which are codified at 10 CFR part 709, but would not preclude the retention of some or all of those regulations through this rulemaking pursuant to the later-enacted section 3152 of the NDAA for FY 2002.

In Part II of this **SUPPLEMENTARY INFORMATION,** DOE reviews background information useful in understanding the existing statutory and regulatory provisions applicable to DOE's current counterintelligence polygraph examination program. In Part III of this **SUPPLEMENTARY INFORMATION,** DOE discusses the basis for today's supplemental proposed regulations, including DOE's evaluation of the NAS Polygraph Review which is entitled ''The Polygraph and Lie Detection.'' In Part IV of this **SUPPLEMENTARY INFORMATION,** DOE provides an overview of today's supplemental proposed regulations with specific references to critical provisions that should be highlighted for the information of potential commenters.

DOE invites interested members of the public to provide their views on the issues in this rulemaking by filing written comments or by attending the public hearing scheduled in this notice. With an open mind, DOE intends carefully to evaluate the public comments received in response to this notice of proposed rulemaking and to respond in a notice of final rulemaking.

II. Background

For more than 50 years, DOE, like its predecessor the Atomic Energy Commission, has had to balance two sets of considerations. On the one hand, we must attract the best minds that we can to do cutting edge scientific work at the heart of DOE's national security mission, and we must allow sufficient dissemination of that work to allow it to be put to the various uses that our national security demands. On the other hand, we must take all reasonable steps to prevent our enemies from gaining access to the work we are doing, lest that work end up being used to the detriment rather than the advancement of our national security. There are no easy answers to the dilemma of how best to reconcile these competing considerations.

The question of whether and to what extent DOE should use the polygraph as a tool for screening individuals for access to our most sensitive information is the latest manifestation of this perennial struggle. This particular chapter begins in 1988, when Congress enacted the Employee Polygraph Protection Act of 1988. That legislation generally restricted employers from using polygraphs to screen potential employees. Congress, however, included three exceptions that are relevant. First, Congress decided that it would not apply any of the legislation's prohibitions to the United States or other governmental employers with respect to their own employees. Second, Congress specifically allowed the Federal government to administer polygraphs to Department of Defense contractors and contractor employees, and Department of Energy contractors and contractor employees in connection with the Department's atomic energy defense activities. And finally, Congress specifically provided that the Federal Government could administer polygraphs to contractors and contractor employees of the intelligence agencies and any other contractor or contractor employee whose duties involve access to top secret information or information that has been designated as within a special access program.

In February 1998, President Clinton issued Presidential Decision Directive-61. In that classified directive, entitled U.S. Department of Energy Counterintelligence Program, the Department was ordered to enhance its protections against the loss or compromise of highly sensitive information associated with certain defense-related programs by considering a variety of improvements to its counterintelligence program. One of these was the use of polygraph examinations to screen individuals with access to this information.

In order to carry out this directive, after initially proceeding through an internal order governing only federal employees, on August 18, 1999 (64 FR 45062), the Department proposed a rule, entitled ''Polygraph Examination Regulation,'' that would govern the use of the polygraph as a screening tool. It proposed that employees at DOE facilities, contractor employees as well as Federal employees, with access to certain classified information and materials, as well as applicants for such positions, be subject to a counterintelligence polygraph before they received initial access to the information and materials and at five-year intervals thereafter.

In the NDAA for FY 2000, Congress directed that the Department administer a counterintelligence polygraph to all Department employees, consultants, and contractor employees in ''high risk programs'' prior to their being given access to the program. Congress specified that these programs were the ''Special Access Programs'' and ''Personnel Security and Assurance Programs.''

On January 18, 2000, the Department finalized essentially the rule it had proposed, which included individuals with access to these programs and others in the screening requirement. Thereafter, on October 30, 2000, Congress enacted the NDAA of FY 2001, which added DOE employees, consultants, and contractor employees in programs that use ''Sensitive Compartmented Information'' and all others already covered by the Department's prior rule to those to whom the polygraph screening mandate applied.

More recently, in the NDAA for FY 2002 (Public Law 107–107), enacted on December 28, 2001, Congress required the Secretary of Energy to carry out, under regulations, a new counterintelligence polygraph program for the Department. Congress directed that the purpose of the new program should be to minimize the potential for release or disclosure of classified data, materials, or information. Congress further directed that the Secretary, in prescribing the regulation for the new program, take into account the results of a not-yet-concluded study being done by the National Academy of Sciences. That study was being conducted pursuant to a contract DOE had entered into with the National Academy of Sciences in November 2000, in which the Department requested the Academy to conduct a review of the existing research on the validity and reliability of polygraph examinations, particularly as used for personnel security screening. Congress directed the Department to propose a new rule regarding polygraphs no later than six months after publication of the NAS study.

The NAS study, entitled The Polygraph and Lie Detection, was published in October 2002 (hereinafter referred to as ''NAS Report'' or ''NAS Study''). The Department published a Notice of Proposed Rulemaking on April 14, 2003 (68 FR 17886). In that Notice, the Department indicated its then-current intent to continue the current polygraph program under a new rule. As the Secretary of Energy said upon release of that proposed rule, he ''concluded that it was appropriate at the present time to'' retain the current system ''in light of the current national security environment, the ongoing military operations in Iraq, and the war on Terrorism.'' At the same time, the Secretary recognized that in the longer term some changes might be appropriate. Therefore, the Department explicitly asked for public comment during a period which ended on June 13, 2003. The Secretary also personally wrote all laboratory directors inviting their comments and views on the proposed rule.

DOE received comments that were mostly critical of the proposal to retain the existing regulations. The comments especially took issue with DOE's proposal, despite the NAS Report, to continue with mandatory employee screening in the absence of an event or other good cause to administer a polygraph examination. Some of the comments recommended random screening as an alternative to mandatory screening. Others complained about the adequacy of the regulatory protections in 10 CFR part 709 against adverse personnel-related action as a result of exclusive reliance on adverse polygraph examination results. Some of the management comments of the DOE weapons laboratories expressed concern about the effect of the counterintelligence polygraph program on employee morale and recruitment. DOE's response to the major issues presented in these critical comments is reflected in parts II and III of this **SUPPLEMENTARY INFORMATION**. DOE invites those who filed comments in response to the April 14, 2003, preliminary notice of proposed rulemaking to reconsider their views in light of the substantial changes to 10 CFR part 709 that DOE has proposed in this notice.

Following the close of the comment period and consideration of public

comments, the Secretary then directed the Deputy Secretary of Energy to conduct a review of the current policy and its implementation history to date, the NAS Report, and the public and internal comments resulting from the Notice of Proposed Rulemaking, and to make recommendations based on his review. The Deputy Secretary worked closely with the Administrator of the National Nuclear Security Administration and the three directors of the nuclear weapons labs. He has discussed the issues with counterintelligence professionals, polygraph experts, and, as part of that review, he has also had access to classified summaries prepared by other Federal agencies regarding their use of polygraph as a screening tool for highly sensitive national security positions.

III. Basis for Supplemental Proposed Rule

The NAS report makes very clear how little we actually know—in a scientific sense—about the theory and practice of polygraphs, either in support of or against the use of polygraphs in a variety of contexts. DOE found many of the NAS's concerns about the ''validity'' of polygraph testing to be well taken. Some employees feel quite strongly that the polygraph is a dangerous tool that either has or will deprive us of the kind of talent that is needed to support our important national security programs. And, yet, DOE proposes to conclude that the utility of polygraphs is strong enough to merit their use in certain situations, for certain classes of individuals, and with certain protections that minimize legitimate concerns expressed by the NAS, employees of the Department and its contractors, and other observers.

DOE is therefore proposing substantial changes to how we use the polygraph in the context of the Department's counterintelligence program. In preparing today's proposal, DOE carefully weighed considerations of fairness to employees with national security objectives. DOE weighed the critical need to protect important classes of national security information against the reality that such information's value is realized in some situations only when shared among talented individuals, without which our national security would suffer. DOE weighed the possibility that individuals who might otherwise be critically important to our national security might not be able to contribute to our security if they choose another type of employment because they object to taking a polygraph exam. DOE weighed the possibility that a polygraph exam that is sensitive enough to raise the likelihood of ''catching'' someone who means to do harm to the United States is also sensitive enough to raise the risk that many ''innocent'' employees will have their lives and employment disrupted by an examination that is either inconclusive or wrongly indicates deception, thereby also potentially depriving the government of their services. Throughout, DOE has been guided by the NAS Report, a study of considerable rigor and integrity both in the sense of what it tells us about what we know and don't know about scientific evidence relating to the polygraph, and in its willingness to make clear the limitations under which the study was conducted.

Perhaps the most difficult issue involves the use of a polygraph as a screening tool, either as a pre-employment test, or as is the case with DOE, as a tool for determining access to certain types of information, programs, or materials. The NAS report points out that the generic nature of the questions asked in the traditional counterintelligence scope exam poses concerns for validity, concerns that are present to a lesser degree when a polygraph exam is focused on a specific set of facts or circumstances. Thus, the NAS report stated, ''we conclude that in populations of examinees such as those represented in the polygraph research literature, untrained in countermeasures, specific-incident polygraph tests can discriminate lying from truth telling at rates well above chance, though well below perfection.'' By contrast, ''polygraph accuracy for screening purposes is almost certainly lower than what can be achieved by specific-incident polygraph tests in the field.''

Adding to the difficulty for public policy makers is the NAS' conclusion that ''virtually all the available scientific evidence on polygraph test validity comes from studies of specific-event investigations'' rather than studies of polygraphs used as a screening tool, and the ''general quality of the evidence for judging polygraph validity is relatively low.'' However, several agencies within the U.S. intelligence community have utilized the counterintelligence scope polygraph for many years as part of both their hiring process and periodic security evaluations of on-board personnel. Those examinations have proved to be very valuable.

Federal agencies deploying the counterintelligence scope polygraph as a screening tool for initial hiring or initial access have detected applicants for classified positions within those agencies who were directed by foreign governments or entities to seek employment with the agencies in order to gain successful penetrations within the various U.S. Government components.

U.S. agencies have also benefited from the utilization of the polygraph screen as part of periodic security evaluations and re-investigations of federal employees and contractor personnel. Such examinations have resulted in multiple admissions in several different areas:

- Knowingly providing classified information to members of foreign intelligence services.
- Involvement in various stages of recruitment efforts by foreign intelligence services.
- Prior unreported contacts with known foreign intelligence officers.
- Efforts by employees to make clandestine contact with foreign diplomatic establishments or foreign intelligence officers.
- Serious contemplation of, or plans to commit, acts of espionage.
- Knowingly providing classified information to foreign nationals and uncleared U.S. persons.

As a result of admissions and subsequent investigations, federal agencies have disrupted on going clandestine relationships between employees/contractors and foreign intelligence officers, and stopped others in their beginning phases, or even before the clandestine relationships began.

If this were the end of the inquiry, it would be a relatively straightforward matter. The probability would be that use of the polygraph screen as one tool for counterintelligence would have a value that demanded its use in the context of access to information the protection of which is critical to our national security, even taking into account questions of employee morale and the resources necessary to sustain such a program. The value of its use in specific-incident investigations would be presumably greater still.

However, that cannot be the end of the inquiry. As the NAS Report makes clear, there are two fundamental issues that must still be confronted: problems associated with examination results that produce ''false positives'' (*i.e.*, where an ''innocent'' person's exam is either inconclusive, or wrongly indicates deception or a significant response meriting further investigation); or ''false negatives'' (*i.e.*, where a ''guilty'' person is judged to have ''passed'' an exam such that no follow up investigation is required). ''False positives'' pose a serious dilemma. They clearly affect the morale of those for whom such a result is reached, and at a certain number can plausibly be expected to affect the

morale of a sizeable portion of the workforce. They risk interrupting the careers of valuable contributors to our nation's defense, if only to fully investigate and clear someone who has not ''passed'' a polygraph. Both ways, therefore, they pose a very serious risk of depriving the United States of the vital services of individuals who may not be easily replaced. They also risk wasting valuable resources, particularly valuable security and counterintelligence resources that could more usefully be deployed in other ways. For all these reasons, therefore, false positives are a serious issue not only as a matter of individual justice but as a matter of the security of the United States.

What this means, in turn, is that the ratio of ''true positives'' to ''false positives'' is a very important consideration in evaluating the polygraph's utility as a screening tool. Unfortunately, we do not really know what that ratio actually is. It largely depends on the accuracy of the polygraph used in this way, as to which, as the NAS Study explains, for the reasons noted above, we do not have enough hard information to make anything more than an educated guess.

Nonetheless, the NAS's conclusion on this point is stark: ''Polygraph testing yields an unacceptable choice * * * Its accuracy in distinguishing actual or potential security violators from innocent test takers is insufficient to justify reliance on its use in employee security screening in federal agencies.''

The NAS analysis underlying this conclusion is very complex and varies somewhat depending on the ''sensitivity threshold'' at which the polygraph is set. There is no need to detail it fully here. However, the bottom line is that DOE found these concerns to be compelling, requiring a satisfactory response in order to continue the use of the polygraph as a counterintelligence tool for screening decisions.

The core of DOE's response is twofold. First, DOE believes that considerations brought out by the NAS Study strongly counsel in favor of ensuring that the types of information that require a screening polygraph in order to obtain access to them are the most critical to our national security, so that we are only incurring the costs that the screening polygraph will inevitably entail in order to protect our most vital information. That has led DOE to propose substantially lowering the number of persons that would be subject to mandatory polygraph screening.

Even in such cases, however, DOE still believes that the costs of allowing bottom-line decisions to be made based solely on a ''positive'' that stands a substantial chance of being a ''false positive'' are unacceptably high. DOE cannot afford them because they risk undermining the very national security goals we hope to attain. The NAS paragraph quoted above actually only goes to the use of the polygraph results as the sole basis for decisionmaking. It does not address the polygraph's use as an investigative lead, to be used in conjunction with other traditional investigative tools. So used, the polygraph seems to be far less problematic because DOE should be able to use these other tools to distinguish the false positives from the true positives. The NAS Report acknowledges that this approach can ameliorate the problems it identifies, noting that ''We believe that any agency that uses polygraphs as part of a screening process should, in light of the inherent fallibility of the polygraph instrument, use the polygraph results only in conjunction with other information, and only as a trigger for further testing and investigation.''

To put the point most simply: DOE knows of no investigative lead that is perfect. Most will identify a substantial number of instances of misconduct or ''false positives'' that do not check out. For example, anonymous tips are the bread and butter of investigations. If an anonymous tipster reports wrongdoing on someone's part that indicates danger to the national security, the report may be true. But it is also possible that the tipster misunderstood something and leapt to an unwarranted conclusion. And it is also possible that the tipster made up or distorted the report in order to slander the subject out of malice, envy, or because of some other grievance or motivation. Anonymity provides a cloak to the tipster that may result in the government's obtaining some true information it otherwise might not get, but it also lowers the costs to the tipster of lying.

Nevertheless, we do not rule out the use of anonymous tips to screen individuals for access to information, or for all kinds of other purposes. Rather, we accept them, but we investigate them. What we do not do, however, is assume they are true and treat them as the sole basis for decisionmaking.

Similarly, techniques in addition to the polygraph are utilized by U.S. Government agencies to determine whether to grant security clearances and determine access to classified information. Those techniques include, among others, national agency checks; credit and criminal checks; and interviews with co-workers. Any of those techniques, standing alone, could produce inaccurate information which, taken on its face without further verification, could lead to adverse consequences to the prospective or current employee. While no individual technique is perfect and without some potential for error, no one has suggested that we should abandon their use, or that we hire people and entrust them with national defense information with no prior checks or reviews whatsoever.

In DOE's view, it is not unreasonable to place the same kind of limited credence in a polygraph result that we place in many other kinds of information that we receive in the course of evaluating whether an individual should be given access to extremely sensitive information. Therefore, DOE believes it should continue to use the polygraph as one tool to assist in making that determination, but that it should not use it as the only tool. That, in turn, leads us to propose retaining the policy in the present rule against taking any ''adverse personnel action'' solely based on the test results of polygraph examinations. Moreover, we are proposing to retain the present policy that no adverse decision on ''access'' to certain information or programs will be made solely on the basis of such test results.

The bottom line is we intend that a polygraph screen operate as a ''trigger'' that may often be useful for subsequent evaluation, but standing alone, to be treated as having no conclusive evidentiary value. In every case of an adverse personnel action, it is DOE policy that such an action or decision is based on other information as well.

There remains the problem of ''false negatives,'' where a polygraph indicates ''no deception'' but the individual is actually being deceptive. The NAS report quite correctly highlights this as also a very real concern. DOE's review of this question persuades it that it is a certainty that any screening polygraph will produce a number of false negatives. These could in theory be significantly diminished by raising the sensitivity threshold of polygraph exams, but that almost certainly raises the numbers of false positives in a population like DOE's where virtually everyone is an honest patriot. Moreover, even this approach will not solve the problem, as we may still end up with a substantial number of false negatives.

Rather, what we must keep in mind is that every ''clearance'' procedure has the problem of ''false negatives.'' It is just as dangerous to simply assume that a successfully completed background check means that we ''know'' the person is loyal to the United States. All that we ''know'' is that we have not found any

evidence of disloyalty. The same should hold for thinking about what it means to ''pass'' a polygraph exam. We actually do not ''know'' that the person is not being deceptive. We simply have not found anything indicating that he or she is. The real life public policy challenge is that we have to make a judgment about how far we go, how many resources we expend, in the search for perfection when it comes to counterintelligence. Quite obviously, considering the many tens of thousands of Americans who have access to information or programs the protection of which is absolutely critical, we are forced to make a probabilistic judgment on how far is enough. The right way to think about this is ''defense in depth.'' One tool alone will not suffice. But many tools, among them the polygraph and other well-known tools, working together can reduce the risk to the greatest extent practical.

IV. Overview of Proposed Regulations

DOE is proposing that the new program, like the current program, be driven by access needs and apply equally to Federal and contractor employees. We will make no distinctions between political appointees or career service professionals. The function or information to which access is sought will be determinative.

DOE is proposing (at proposed section 709.3(a)) to retain a mandatory CI evaluation program including polygraph screening principally for individuals with ''regular and routine access'' to the most sensitive information. (The term ''regular and routine access'' is defined at proposed section 709.2.) The proposed rule, like the current regulation, would provide for a mandatory counterintelligence (CI) evaluation (hereafter referred to as CI evaluation), including a CI-scope polygraph examination prior to initial access being granted, as well as periodic CI evaluations at intervals not to exceed five years.

Overall, DOE's proposal would narrow the range of information, access to which will trigger mandatory screening as compared to the potential scope of the program under the current legislation. The approach in today's proposal would have the effect of reducing the number of individuals subject to mandatory screening from in excess of potentially 20,000 under the current legislation to approximately 4,500 under this new program.

In addition, DOE is proposing that some elements of the mandatory screening population remain essentially the same as under the current regulation. For example: all counterintelligence employees; all employees in the Headquarters Office of Intelligence and at the Field Intelligence Elements; and all employees in DOE Special Access Programs (and non-DOE Special Access Programs if a requirement of the program sponsor) will be included in the mandatory screening program. These employees would continue to be subject to mandatory screening because they have routine access to highly sensitive information, such as foreign intelligence information and other extremely close-hold and compartmented information.

DOE has searched for a test to identify the types of information that on balance would overcome the very real concerns about the validity of the polygraph screen. Most would agree that the polygraph should be reserved for only those programs or information, the protection of which is the most critical. As it happens, we have a well understood test of how to define the damage disclosure of certain information would present: the current classification levels of Confidential, Secret, and Top Secret. There are additional categories that are also important, but it seems that the definition of Top Secret is a better way to capture the information most precious to us: ''information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security''.

Thus, DOE is proposing including in the mandatory screening program those employees with ''regular and routine access'' to all DOE-originated ''Top Secret'' information, including Top Secret ''Restricted Data'' and Top Secret ''National Security Information.'' (The terms in quotation marks are defined at proposed section 709.2.) Top Secret Restricted Data is a clearly distinguishable criterion that identifies the weapons community's most sensitive information assets. Other non-weapons-related Top Secret information, categorized as Top Secret National Security Information, although not dealing with nuclear weapons, includes our most sensitive national security information. This category would not include everyone with a ''Q'' or a Top Secret clearance, nor would it include all weapons scientists; it would include only those employees who require continuing, routine access to Top Secret RD or other DOE-originated Top Secret information. This is a fairly small population.

The proposed rule also would include authority for certain managers, with input from the Office of Counterintelligence and subject to the approval by the Secretary, to include additional individuals within their offices or programs in the mandatory screening program. This authority would allow designation of individuals within the Office of the Secretary, the National Nuclear Security Administration, the Office of Security, the Office of Emergency Operations, the Office of Independent Oversight and Performance Assurance, and the Human Reliability Program (HRP) under 10 CFR part 712. (See proposed section 709.3(a)(6) and (f).) The criteria for conducting a risk assessment are set forth at section 709.3(e). Those criteria are: access on a non-regular and non-routine basis to top secret restricted data or top secret national security information or the nature and extent of access to other classified information; unescorted or unrestricted access to significant quantities or forms of special nuclear materials; and any other factors concerning the employee's responsibilities that are relevant to determining risk of unauthorized disclosure of classified information or materials.

DOE is proposing not to designate for mandatory CI evaluations screening all individuals in the HRP. The NDAA for FY 2000 originally mandated that everyone in this program be subject to a screening polygraph, and the NDAA for FY 2001 retained that mandate.

The NDAA for FY 2002, however, directs that the focus of DOE's polygraph program be the protection of classified data, materials or information. The HRP applies to individuals primarily not by reason of their access to classified information but because of their responsibilities for nuclear materials. Many, if not most, of the HRP individuals do not have routine access to the most sensitive classified information.

DOE envisions, as one element of the new program, that employees designated for mandatory screening under the new regulation would be allowed to retain access to classified information or materials pending scheduling of their first CI evaluation.

We now turn to an entirely new proposed element of the overall program—the random screening program. We have identified a universe of employees whose level and frequency of access, while not requiring mandatory screening, nevertheless warrants some additional measure of deterrence against damaging disclosures. (See proposed section 709.3(b).)

In reviewing the public policy dimensions of the polygraph, one is

struck by the ''either-or'' aspect of the debate: either you are subject to a polygraph, or you are not. This strikes DOE as too simplistic. The types of information we are concerned with do not easily fall into categories where either we fully deploy every tool we have to defend against disclosure or we do nothing. The classification regime itself acknowledges that there is a continuum, and that these determinations are based on less science and more judgment than is often admitted. Nonetheless, the problem of targeting is perhaps unique to DOE facilities, and especially our three weapons labs, in a way not present elsewhere in our national security complex. Nowhere else in America can someone—in one location—find not only our most sensitive nuclear weapons secrets, but secrets addressing other weapons of mass destruction, and special nuclear material.

There are many ways to deter and detect such targeting, and the security and counterintelligence functions at DOE command the full attention of DOE's leadership, substantial resources, large and highly trained protective forces, and security and access controls that are too numerous to list here. Nonetheless, we will do everything we can to strengthen our ability to detect and deter activities inimical to our interests. Thus, as a policy matter, unless there are very compelling countervailing considerations, we should pursue even modest additions to the arsenal of tools we deploy to deter dissemination of this information to our enemies given the potentially grave consequences of failure.

It is noteworthy that the NAS report, while questioning the validity of polygraph screens and their value in ''detection,'' also stated that ''polygraph screening may be useful for achieving such objectives as deterring security violations, increasing the frequency of admissions of such violations, [and] deterring employment applications from potentially poor security risks.''

As the NAS report notes, ''the value, or utility, of polygraph testing does not lie only in its validity for detecting deception. It may have a deterrent value * * *'' And, as the NAS report also notes, ''predictable polygraph testing (*e.g.*, fixed-interval testing of people in specific job classifications) probably has less deterrent value than random testing.'' This leads DOE to conclude that it is appropriate in some instances to include some form of screening beyond that routinely required to obtain and maintain access to classified information or materials that makes some use of the deterrent value of the polygraph. The random screening program is intended to meet this need and to supplement the mandatory screening program. Under the random screening portion of the program, CI evaluations would not be a condition of initial entry nor would individuals with access to the information at issue be subject to mandatory polygraphs at specific intervals. However, they would be subject to random selection for CI evaluations at any time, at any frequency. In essence, even though it is possible that an individual may never actually be selected through the random process, the individual could be subject to a (random) CI evaluation at any time, even if the individual recently completed one.

While the overall goal is one of deterrence, an associated benefit is that the random program serves to reduce the number of individuals in the mandatory program, allowing us to focus our resources more wisely. Thus, it will be DOE's policy to fashion a random CI evaluation program including polygraph that achieves the objectives of deterrence with the minimum reasonable percentage or number of individuals to which it applies. Since we estimate the total number of individuals who would be eligible for the random CI evaluations including polygraph to be small, the use of a minimum percentage means the total number of random polygraphs in any given year would be a much lower number. Proposed section 709.3(b) lists individuals whose occasional access to classified information or materials would merit screening. Again, the population associated with routine access to such information will not encompass the entire population of ''Q'' cleared individuals.

In addition, due to the interconnectedness of DOE sites and cyber networks and the volume of sensitive unclassified information, we are already taking steps to apply additional security controls (clearance requirements, segregation of duties, two-person rules, etc.) to system administrators of unclassified systems.

In addition to the mandatory and random screening programs, DOE is proposing a provision for conducting ''specific-incident'' polygraph examinations in response to specific facts or circumstances with potential counterintelligence implications with a defined foreign nexus. (See proposed section 709.3(c).) That recommendation also grows out of the NAS Report, which noted that this kind of use of the polygraph is the one for which the existing scientific literature provides the strongest support. The proposed rule also would provide for employee-requested polygraph examinations in the context of a specific incident. (See proposed section 709.3(c).)

The proposed rule would not retain the provision in the existing regulations concerning the use of polygraph examinations for the Accelerated Access Authorization Program (AAAP). Since AAAP is related exclusively to expedited interim access authorizations rather than to DOE's Counterintelligence Evaluation Program, it should not be covered by part 709. Nevertheless, DOE did undertake a review of the use of polygraph examinations as part of the AAAP, in light of the NAS report, to determine if it was unduly reliant on such examinations in granting interim access authorizations. DOE's review found that there are sufficient checks and balances in place that the continued use of polygraph examinations, together with the other components of the AAAP, is appropriate. Likewise, the proposed rule deletes the general provision in the existing regulations regarding employee requested polygraphs.

As the discussion above makes clear, the Department is strongly committed to maximizing protections against potential errors and adverse consequences and safeguarding the privacy of the employees who are subject to CI evaluations. Therefore the proposed rule would retain and enhance the protections already contained in the current regulation. The provisions we would retain include: written notification by DOE and written consent from the employee are required before a polygraph examination can be administered; a prohibition against recording a refusal to submit to a polygraph examination in an employee's personnel file; audio and video recordings of polygraph examination sessions would be made to protect both the employee and the polygrapher; all polygraph examination records and reports would be maintained in a system of records established under the Privacy Act; and strict qualification standards and standards of conduct for polygraphers would be established and enforced. Neither the polygrapher nor the Office of Counterintelligence would have the authority to make a decision to grant or deny access to information covered by part 709. That decision would be made by the Program Manager or the Secretary. The polygraph examination would be limited to topics concerning the individual's involvement in espionage, sabotage, terrorism, unauthorized disclosure of classified information, unauthorized foreign

contacts, and deliberate damage to or malicious misuse of a U.S. government information or defense system. The examiner would not be permitted to ask ''lifestyle'' questions, *e.g.*, drugs, crimes, and falsification of application.

Perhaps the most important aspect of these safeguards is how we address the problem of ''false positives.'' Assuming we adhere to the difficult policy choice that the continued use of polygraphs as both a screening tool and for resolving specific incidents is appropriate, we believe that it is absolutely necessary to ensure that we minimize to the greatest extent possible any morale effects of the polygraph, and do everything we can to prevent ''false positives'' from producing an unfair result to an employee.

Limiting the population of those subject to mandatory screening polygraphs is the most important step we can take to limit these kinds of problems. In addition, however, we are proposing a few improvements to the current rule. First, we would clarify that the sole purpose for which we use the polygraph as a screening tool is to assist us in making determinations about whether an individual may be given access to specific categories of highly sensitive information. Otherwise, DOE does not use it to make employment decisions at all, except to the extent that access to this information may be a critical element of someone's job.

The proposed rule also would make clear that it is DOE's policy not to base a denial of access solely on the results of a polygraph exam. (See proposed section 709.25(a).) This would be consistent with the NAS report's recommendation: ''We believe that any agency that uses polygraphs as part of a screening process should, in light of the inherent fallibility of the polygraph instrument, use the polygraph results only in conjunction with other information, and only as a trigger for further testing and investigation.''

The proposed rule also would improve the process for making decisions to grant, continue, or deny access to these high-risk programs by providing for a counterintelligence evaluation review board, including senior DOE officials, that may be convened by the Director of the Office of Counterintelligence to consider the results of counterintelligence evaluations that are not dispositive and to solicit the individual recommendations of the board members. The board could include the appropriate weapons laboratory director if the access determination involves a laboratory employee.

Because the policy choices discussed above lead to the conclusion that the polygraph should be just one tool of many, the proposed rule would make clear that polygraphs are just one element to be used in counterintelligence evaluations. The current rule refers to review of personnel security files and personal interviews in conjunction with the polygraph. The proposed rule would broaden this reference to provide that DOE may when appropriate employ other techniques, such as review of financial and credit information, net worth analyses, analyses of foreign travel and foreign contacts and connections, and other relevant information. Any such review by OCI will be conducted in accordance with Executive Order 12333, the DOE ''Procedures for Intelligence Activities,'' and other relevant laws, guidelines and authorities as may be applicable with respect to such matters.

In addition to a wider array of tools, better tools are needed to increase the reliability and validity of screening processes. The NAS report called for basic and applied scientific research into improved security screening techniques, and suggested that such an effort could be devoted in part to developing knowledge to put the polygraph technique on a firmer scientific foundation, which could strengthen its acceptance as a tool for detecting and deterring security threats. We have also identified a need for basic research into improved screening technologies, including but not limited to psychological and behavioral assessment techniques. It may be, as the NAS report suggests, that this research is best conducted under the auspices of an organization other than an agency that invests considerable resources in a counterintelligence polygraph program. DOE stands ready to lead or assist in such research.

V. Regulatory Review

A. National Environmental Policy Act

The proposed rule would retain the existing procedures for counterintelligence evaluations to include polygraph examinations and therefore will have no impact on the environment. DOE has determined that this rule is covered under the Categorical Exclusion in DOE's National Environmental Policy Act regulations in paragraph A.5 of appendix A to subpart D, 10 CFR part 1021, which applies to rulemakings amending an existing regulation that does not change the environmental effect of the regulations being amended. Accordingly, neither an environmental assessment nor an environmental impact statement is required.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act, 5 U.S.C. 601–612, requires preparation of an initial regulatory flexibility analysis for every rule that must be proposed for public comment, unless the agency certifies that the rule, if promulgated, will not have a significant economic impact on a substantial number of small entities. This rulemaking will not directly regulate small businesses or small governmental entities. It will apply principally to individuals who are employees of, or applicants for employment by, some of DOE's prime contractors, which are large businesses. There may be some affected small businesses that are subcontractors, but the rule will not impose unallowable costs. Accordingly, DOE certifies that the proposed rule, if promulgated, will not have a significant economic impact on a substantial number of small entities.

C. Paperwork Reduction Act

DOE has determined that this proposed rule does not contain any new or amended record keeping, reporting or application requirements, or any other type of information collection requirements that require the approval of the Office of Management and Budget (OMB) under the Paperwork Reduction Act, 44 U.S.C. 3501, *et seq*. The OMB has defined the term ''information'' to exclude certifications, consents, and acknowledgments that entail only minimal burden (5 CFR 1320.3(h)(1)).

D. Unfunded Mandates Reform Act of 1995

The Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1531 *et seq.*, requires a Federal agency to perform a detailed assessment of the costs and benefits of any rule imposing a Federal mandate with costs to state, local, or tribal governments, or to the private sector of $100 million or more. The proposed rule does not impose a Federal mandate requiring preparation of an assessment under the Unfunded Mandates Reform Act of 1995.

E. Treasury and General Government Appropriations Act, 1999

Section 654 of the Treasury and General Government Appropriations Act of 1999, (Public Law 105–277), requires Federal agencies to issue a Family Policymaking Assessment for any proposed rule that may affect family well being. This proposed rule will not have any impact on the autonomy or

integrity of the family as an institution. Accordingly, DOE has concluded that it is not necessary to prepare a Family Policymaking Assessment.

F. Executive Order 12866

In accordance with Executive Order 12866, the rule has been determined to be significant and has been reviewed by the Office of Management and Budget.

G. Executive Order 12988

Section 3(a) of Executive Order 12988, 61 FR 4729 (February 7, 1996) imposes on executive agencies the general duty to adhere to the following requirements: (1) Eliminate drafting errors and ambiguity; (2) write regulations to minimize litigation; and (3) provide a clear legal standard for affected conduct rather than a general standard, and promote simplification and burden reduction. Section 3(b) of Executive Order 12988 specifically requires that executive agencies make every reasonable effort to ensure that the regulation: (1) Clearly specifies the preemptive effect, if any; (2) clearly specifies any effect on existing Federal law or regulation; (3) provides a clear legal standard for affected conduct while promoting simplification and burden reduction; (4) specifies the retroactive effect, if any; (5) adequately defines key terms; and (6) addresses other important issues affecting clarity and general draftsmanship under any guidelines issued by the Attorney General. Section 3(c) of Executive Order 12988 requires executive agencies to review regulations in light of applicable standards in section 3(a) and section 3(b) to determine whether they are met or it is unreasonable to meet one or more of them. DOE has completed the required review and determined that, to the extent permitted by law, this proposed rule meets the relevant standards of Executive Order 12988.

H. Executive Order 13084

Under Executive Order 13084, 63 FR 27655 (May 19, 1998), DOE may not issue a discretionary rule that significantly or uniquely affects Indian tribal governments and imposes substantial direct compliance costs. This proposed rulemaking would not have such effects. Accordingly, Executive Order 13084 does not apply to this rulemaking.

I. Executive Order 13132

Executive Order 13132, 64 FR 43255 (August 10, 1999), requires agencies to develop an accountable process to ensure meaningful and timely input by state and local officials in the development of regulatory policies that have ''federalism implications.'' Policies that have federalism implications are defined in the Executive Order to include regulations that have ''substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.'' On March 14, 2000, DOE published a statement of policy describing the intergovernmental consultation process it will follow in the development of such regulations (65 FR 13735). DOE has examined this proposed rule and determined that it would not have a substantial direct effect on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. No further action is required by the Executive Order.

J. Executive Review Under Order 13211

Executive Order 13211 (Actions Concerning Regulations That Significantly Affect Energy, Supply, Distribution, or Use), 66 FR 28355 (May 22, 2001) requires preparation and submission to OMB of a Statement of Energy Effects for significant regulatory action under Executive Order 12866 that are likely to have a significant adverse effect on the supply, distribution, or use of energy. This rulemaking, although significant, will not have such an effect. Consequently, DOE has concluded that there is no need for a Statement of Energy Effects.

K. Treasury and General Government Appropriations Act, 1999

The Treasury and General Government Appropriations Act, 2001 (44 U.S.C. 3516, note) provides for agencies to review most disseminations of information to the public under guidelines established by each agency pursuant to general guidelines issues by OMB. OMB's guidelines were published at 67 FR 8452 (February 22, 2001), and DOE's guidelines were published at 67 FR 62446 (October 7, 2002). DOE has reviewed this notice of proposed rulemaking under the OMB and DOE guidelines, and has concluded that it is consistent with applicable policies in those guidelines.

VI. Opportunity for Public Comment

A. Written Comments

Interested members of the public are invited to participate in this proceeding by submitting data, views, or comments on this proposed rule. Ten copies of written comments should be submitted to the address indicated in the **ADDRESSES** section of this notice of proposed rulemaking. Comments should be identified on the outside of the envelope and on the comments themselves with the designation ''Counterintelligence Evaluation Regulation, Docket No. CN–03–RM–01.'' If anyone wishing to provide written comments is unable to provide ten copies, alternative arrangements can be made in advance with the DOE. All comments received on or before the date specified at the beginning of this notice, and other relevant information before final action is taken on the proposed rule, will be considered.

All submitted comments will be available for public inspection as part of the administrative record on file for this rulemaking in the DOE Freedom of Information Reading Room at the address indicated in the **ADDRESSES** section of this notice of proposed rulemaking. Pursuant to the provisions of 10 CFR 1004.11, anyone submitting information or data that he or she believes to be confidential and exempt by law from public disclosure should submit one complete copy of the document, as well as two copies, if possible, from which the information has been deleted. DOE will make its determination as to the confidentiality of the information and treat it accordingly.

B. Public Hearing

You will find the time and place of the public hearing listed at the beginning of this notice of proposed rulemaking. We invite any person who has an interest in today's notice of proposed rulemaking, or who is a representative of a group or class of persons that has an interest in these issues, to request an opportunity to make an oral presentation. If you would like to speak at the public hearing, please notify Andi Kasarsky at (202) 586–3012. You may also send your notification by mail or e-mail to the address given in the **ADDRESSES** section at the beginning of this notice of proposed rulemaking. The person making the request should briefly describe the nature of the interest in the rulemaking, and provide a telephone number for contact.

DOE will designate a DOE official to preside at the public hearing. The public hearing will not be a judicial or evidentiary-type hearing, but DOE will conduct it in accordance with 5 U.S.C. 553 and section 501 of the Department of Energy Organization Act (42 U.S.C. 7191). Oral statements should be limited to 10 minutes. At the conclusion of all initial oral statements, each person who

has made an oral statement will be given the opportunity, if he or she so desires, to make a rebuttal or clarifying statement. The statements will be given in the order in which the initial statements were made and will be subject to time limitations. Only those conducting the hearing may ask questions.

DOE will prepare a transcript of the hearing. DOE will retain the transcript and other records of this rulemaking and make them available for inspection in DOE's Freedom of Information Reading Room, as provided at the beginning of this notice of proposed rulemaking. Any person may purchase a copy of the transcript from the transcribing reporter.

The presiding official will announce any further procedural rules needed for the proper conduct of the hearing.

List of Subjects

10 CFR Part 709

Lie detector tests, Privacy.

10 CFR Part 710

Administrative practice and procedure, Classified information, Government contracts, Nuclear materials.

Issued in Washington, DC, on December 30, 2004.

Stephen W. Dillard,

Director, Office of Counterintelligence.

For the reasons stated in the preamble, DOE hereby proposes to amend chapter III of title 10 of the Code of Federal Regulations as follows:

1. Part 709 is revised to read as follows:

PART 709—COUNTERINTELLIGENCE EVALUATION PROGRAM

Subpart A—General Provisions

Sec.

Subpart B—CI Evaluation Protocols and Protection of National Security

Subpart C—Safeguarding Privacy and Employee Rights

Subpart D—Polygraph Examination and Examiner Standards

Authority: 42 U.S.C. 2011, *et seq.*, 7101, *et seq.*, 7144b, *et seq.*, 7383h–1; 50 U.S.C. 2401, *et seq.*

Subpart A—General Provisions

§ 709.1 Purpose.

This part:

(a) Describes the categories of individuals who are subject for counterintelligence evaluation processing;

(b) Provides guidelines for the counterintelligence evaluation process, including the use of counterintelligence-scope polygraph examinations, and for the use of event-specific polygraph examinations; and

(c) Provides guidelines for protecting the rights of individual DOE employees and DOE contractor employees subject to this part.

§ 709.2 Definitions.

For purposes of this part:

Access authorization means an administrative determination under the Atomic Energy Act of 1954, Executive Order 12968, or 10 CFR part 710 that an individual is eligible for access to classified matter or is eligible for access to, or control over, special nuclear material.

Adverse personnel action means:

(1) With regard to a DOE employee, the removal, suspension for more than 14 days, reduction in grade or pay, or a furlough of 30 days or less as described in 5 U.S.C. chapter 75; or

(2) With regard to a contractor employee, the discharge, discipline, or denial of employment or promotion, or any other discrimination in regard to hire or tenure of employment or any term or condition of employment.

Contractor means any industrial, educational, commercial, or other entity, assistance recipient, or licensee, including an individual that has executed an agreement with DOE for the purpose of performing under a contract, license, or other agreement, and including any subcontractors of any tier.

Counterintelligence or CI means 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.

Counterintelligence evaluation or CI evaluation means the process, including a counterintelligence scope polygraph examination, employed by the Office of Counterintelligence to make recommendations as to whether certain employees should have access to information or materials protected by this part.

Counterintelligence program office means the Office of Counterintelligence established under section 215 of the Department of Energy Organization Act (and any successor office to which that office's duties and authorities may be reassigned) and the Office of Defense Nuclear Counterintelligence established by section 3232 of the National Defense Authorization Act for Fiscal Year 2000 (and any successor office to which that office's duties and authorities may be reassigned).

Counterintelligence-scope or CI-scope polygraph examination means a polygraph examination using questions reasonably calculated to obtain counterintelligence information, including questions relating to espionage, sabotage, terrorism, unauthorized disclosure of classified information, deliberate damage to or malicious misuse of a United States Government information or defense system, and unauthorized contact with foreign nationals.

Covered person means an applicant for DOE or contractor employment, a DOE employee, a DOE contractor employee, and an detailee to DOE from another agency.

DOE means the Department of Energy including the National Nuclear Security Administration (NNSA).

Foreign nexus means specific indications that a subject DOE employee or contractor employee is or may be engaged in clandestine or unreported

relationships with foreign powers, organizations or persons, or international terrorists; contacts with foreign intelligence services; or other hostile activities directed against DOE facilities, property, personnel, programs or contractors by or on behalf of foreign powers, organizations or persons, or international terrorists.

Human reliability program means the program under 10 CFR part 712;

Intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons.

Local commuting area means the geographic area that usually constitutes one area for employment purposes. It includes any population center (or two or more neighboring ones) and the surrounding localities in which people live and can reasonably be expected to travel back and forth daily to their usual employment.

Materials means any ''nuclear explosive'' as defined in 10 CFR 712.3, and any ''special nuclear material,'' hazardous ''source material,'' and hazardous ''byproduct material'' as those terms are defined by the Atomic Energy Act of 1954 (42 U.S.C. 2014).

National security information means information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

NNSA means DOE's National Nuclear Security Administration.

No opinion means an evaluation of a polygraph test by a polygraph examiner in which the polygraph examiner cannot render an opinion.

No significant response means an opinion indicating that the analysis of the polygraph charts revealed no consistent, significant, timely physiological responses to the relevant questions.

Polygraph examination means all activities that take place between a Polygraph Examiner and an examinee (person taking the test) during a specific series of interactions, including the pretest interview, the use of the polygraph instrument to collect physiological data from the examinee while presenting a series of tests, the test data analysis phase, and the post-test phase.

Polygraph examination records means all records of the polygraph examination, including the polygraph report, audio-video recording, and the polygraph consent form.

Polygraph instrument means a diagnostic instrument used during a polygraph examination, which is capable of monitoring, recording and/or measuring at a minimum, respiratory, electrodermal, and cardiovascular activity as a response to verbal or visual stimuli.

Polygraph report means a document that may contain identifying data of the examinee, a synopsis of the basis for which the examination was conducted, the relevant questions utilized, and the examiner's conclusion.

Polygraph test means that portion of the polygraph examination during which the polygraph instrument collects physiological data based upon the individual's responses to questions from the examiner.

Program Manager means a DOE official designated by the Secretary or the Head of a DOE Element to make an access determination under this part.

Random means a statistical process whereby eligible employees have an equal probability of selection for a CI evaluation each time the selection process occurs.

Regular and routine means access without further permission or individuals who access such information more than two times per quarter.

Relevant questions are those questions used during the polygraph examination that pertain directly to the issues for which the examination is being conducted.

Restricted data means all data concerning 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, but does not include data declassified or removed from the restricted data category pursuant to section 142 of the Atomic Energy Act of 1954.

Secret means the security classification that is applied to DOE-generated information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Secretary means the Secretary of Energy or the Secretary's designee.

Significant response means an opinion that the analysis of the polygraph charts revealed consistent, significant, timely physiological responses to the relevant questions.

Special Access Program or SAP means a program established under Executive Order 12958 for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Suspend means temporarily to withdraw an employee's access to information or materials protected under § 709.3 of this part.

System Administrator means any individual who has privileged system, data, or software access that permits that individual to exceed the authorization of a normal system user and thereby override, alter, or negate integrity verification and accountability procedures or other automated and/or technical safeguards provided by the systems security assets for normal users.

Top Secret means the security classification that is applied to DOE-generated information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Unresolved issues means an opinion by a CI evaluator that the analysis of the information developed during a CI evaluation remains inconclusive and needs further clarification before a CI access recommendation can be made.

§ 709.3 Individuals subject to a CI evaluation and polygraph.

(a) *Mandatory CI evaluation.* Except as provided in § 709.5 of this part with regard to waivers, a CI evaluation, including a CI-scope polygraph examination, is required for any covered person who will have or has access to classified information or materials protected under this paragraph. Such an examination is required for covered persons who are incumbent employees at least once every five years and at intervals determined through random selection. This paragraph applies to covered persons:

(1) In a counterintelligence program office (or with programmatic reporting responsibility to a counterintelligence program office) because of access to classified information, or counterintelligence information, sources, and methods;

(2) In the DOE Office of Intelligence and all DOE field intelligence elements because of the direct, unrestricted nature of their employees' access to raw classified intelligence information;

(3) With access to information that is protected within a non-intelligence Special Access Program (SAP) designated by the Secretary;

(4) With regular and routine access to Top Secret Restricted Data;

(5) With regular and routine access to Top Secret National Security Information; and

(6) Designated, with approval of the Secretary, on the basis of a risk

assessment consistent with paragraph (e) and (f) of this section, by a Program Manager for the following DOE offices and programs (and any successors to those offices and programs): the Office of the Secretary; the Human Reliability Program; the National Nuclear Security Administration; the Office of Independent Oversight and Performance Assurance; the Office of Security; and the Office of Emergency Operations (OEO).

(b) *Random CI evaluation.* Except as provided in § 709.5 of this part with regard to waivers, DOE may require a CI evaluation, including a CI-scope polygraph examination, of covered persons who are incumbent employees selected on a random basis from the following:

(1) All employees in the Office of Security because of their access to classified information;

(2) All employees in the Office of Emergency Operations (OEO or any successor office) including DOE field offices or contractors who support OEO because of their access to classified information;

(3) All employees in the Office of Independent Oversight and Performance Assurance (or any successor office) because of access to classified information regarding the inspection and assessment of safeguards and security functions, including cyber security, of the DOE;

(4) All employees with regular and routine access to classified information concerning: the design and function of nuclear weapons use control systems, features, and their components (currently designated as Sigma 15); vulnerability of nuclear weapons to deliberate unauthorized nuclear detonation (currently designated as Sigma 14); and improvised nuclear device concepts or designs; and

(5) Any system administrator with access to a system containing classified information, as identified by the DOE or NNSA Chief Information Officer.

(c) *Specific incident polygraph examinations.* In response to specific facts or circumstances with potential counterintelligence implications with a defined foreign nexus, the Director of the Office of Counterintelligence may require a covered person with access to DOE classified information or materials to consent to and take an event-specific polygraph examination. Except as otherwise determined by the Secretary, on the recommendation of the appropriate Program Manager, if a covered person with access to DOE classified information or materials refuses to consent to or take a polygraph examination under this paragraph, then the Director of the Office of Counterintelligence will direct the denial of access (if any) to classified information and materials protected under paragraphs (a) and (b) of this section, and will refer the matter to the Office of Security for a review of access authorization eligibility under 10 CFR part 710. In addition, in the circumstances described in this paragraph, any covered person with access to DOE classified information or material may request a polygraph examination.

(d) *Risk assessment.* For the purpose of deciding whether to designate or remove employees for mandatory CI evaluations under paragraph (a)(6) of this section, Program Managers may consider:

(1)Access on a non-regular and non-routine basis to top secret restricted data or top secret national security information or the nature and extent of access to other classified information;

(2) Unescorted or unrestricted access to significant quantities or forms of special nuclear materials; and

(3) Any other factors concerning the employee's responsibilities that are relevant to determining risk of unauthorized disclosure of classified information or materials.

(e) Based on the risk assessments conducted under paragraph (e) of this section and in consultation with the Director of the Office of Counterintelligence, the Program Manager shall provide recommendations as to positions to be designated or removed under paragraph (a)(6) of this section for approval by the Secretary. Recommendations shall include a summary of the basis for designation or removal of the positions and of the views of the Director of Counterintelligence as to the recommendations.

(f) Not less than once every calendar year quarter, the responsible Program Manager must provide a list of all incumbent personnel covered above in paragraphs (a) and (b) of this section to the Director of the Office of Counterintelligence.

§ 709.4 Notification of a CI evaluation.

(a) If a polygraph examination is scheduled, DOE must notify the individual, in accordance with § 709.21of this part.

(b) Any job announcement or posting with respect to any position with access to classified information or materials protected under § 709.3(a) and (b) of this part must indicate that the selection of an individual for the position (§ 709.3(a)) or retention in that position (§ 709.3(a) and (b)) may be conditioned upon his or her successful completion of a CI evaluation, including a CI-scope polygraph examination.

(c) The Office of Counterintelligence provides advance notice to the affected Program Manager and laboratory/site/facility director of the individuals who are included in any random examinations that are administered in accordance with provisions at § 709.3(b).

§ 709.5 Waiver of polygraph examination requirements.

(a) *General.* The CI-scope polygraph examination requirement under § 709.3 of this part does not apply to:

(1) Any individual for whom the Director of the Office of Counterintelligence gives a waiver, based upon certification from another Federal agency that the individual has successfully completed a full scope or CI-scope polygraph examination administered within the previous five years;

(2) Any individual who is being treated for a medical or psychological condition that, based upon consultation with the individual and appropriate medical personnel, the Secretary or the Director of the Office of Counterintelligence determines would preclude the individual from being tested; or

(3) Any individual for whom the Secretary gives a written waiver in the interest of national security.

(b) *Submission of waiver requests.* Each request submitted under § 709.5(a)(2) shall assert the basis or waiver sought and shall be submitted, in writing, to the Director of the Office of Counterintelligence at the following address: U.S. Department of Energy, Attn: Director, Office of Counterintelligence, 1000 Independence Avenue, SW., Washington, DC 20585.

(c) *Disposition of waiver requests.* Decisions on waivers are issued in writing. If a waiver request is approved, the notification contains information regarding the duration of the waiver and any other relevant instructions, as deemed appropriate. If the waiver is denied, the notification explains the basis for the denial.

(d) *Reconsideration rights.* If a waiver is denied by the Director of the Office of Counterintelligence, the notification informs the candidate that a request for reconsideration by the Secretary of Energy may be filed within 30 days of receipt of the decision.

Subpart B—CI Evaluation Protocols and Protection of National Security

§ 709.10 Scope of a counterintelligence evaluation.

At a minimum, a counterintelligence evaluation consists of a counterintelligence-scope polygraph examination and a counterintelligence-based review of the covered individual's personnel security file. As set forth in § 709.15(b) and (c) of this part, a counterintelligence evaluation may also include other pertinent measures to address and resolve counterintelligence issues in accordance with Executive Order 12333, the DOE ''Procedures for Intelligence Activities,'' and other relevant laws, guidelines and authorities, as applicable.

§ 709.11 Topics within the scope of a polygraph examination.

(a) DOE may ask questions in a specific incident polygraph examination that are appropriate to a CI-scope examination or that are relevant to the counterintelligence concerns with a defined foreign nexus.

(b) A CI-scope polygraph examination is limited to topics concerning the individual's involvement in espionage, sabotage, terrorism, unauthorized disclosure of classified information, unauthorized foreign contacts, and deliberate damage to or malicious misuse of a U.S. government information or defense system.

(c) DOE may not ask questions that:

(1) Probe an individual's thoughts or beliefs;

(2) Concern conduct that has no CI implication with a defined foreign nexus; or

(3) Concern conduct that has no direct relevance to a CI evaluation.

§ 709.12 Defining polygraph examination questions.

The examiner determines the exact wording of the polygraph questions based on the examiner's pretest interview of the individual, the individual's understanding of the questions, established test question procedures from the Department of Defense Polygraph Institute, and other input from the individual.

§ 709.13 Implications of refusal to take a polygraph examination.

(a) Subject to § 709.14 of this part, an individual may refuse to take a polygraph examination pursuant to § 709.3 of this part, and an individual being examined may terminate the examination at any time.

(b) If an individual terminates a CI-scope examination prior to the completion of the examination, DOE may treat that termination as a refusal to take a polygraph examination under § 709.14.

§ 709.14 Consequences of a refusal to complete a CI evaluation including a polygraph examination.

(a) If an individual is an applicant for employment or assignment or a potential detailee and the individual refuses to complete a CI evaluation including a polygraph examination required by this part as an initial condition of access, DOE and its contractors must refuse to employ, assign, or detail that individual to the identified position.

(b) If an individual is an incumbent employee subject to a CI evaluation including a polygraph examination under § 709.3(a), (b), or (c), and the individual refuses to complete a CI evaluation, DOE and its contractors must deny that individual access to classified information and materials protected under § 709.3(a) and (b) and may take other actions consistent with the denial of access, including administrative review of access authorization under 10 CFR part 710. If the individual is a DOE employee, DOE may reassign or realign the individual's duties, or take other action, consistent with that denial of access and applicable personnel regulations.

(c) If a DOE employee refuses to take a CI polygraph examination, DOE may not record the fact of that refusal in the employee's personnel file.

§ 709.15 Processing counterintelligence evaluation results.

(a) *General.* A Counterintelligence Evaluation under this part consists of three elements:

(1) CI-scope polygraph examination;

(2) Review of the personnel security file; and

(3) Review of other relevant information available to DOE in accordance with applicable guidelines and authorities.

(b) If the polygraph examination and reviews under paragraph (a) of this section present unresolved foreign nexus issues that raise significant questions about the individual's access to classified information or materials protected under § 709.3 of this part that justified the counterintelligence evaluation, DOE may undertake a more comprehensive CI evaluation that may, in appropriate circumstances, include evaluation of financial, credit, travel, and other relevant information to resolve any identified issues. Participation by OCI in any such evaluation is subject to Executive Order 12333, the DOE ''Procedures for Intelligence Activities,'' and other relevant laws, guidelines, and authorities as may be applicable with respect to such matters.

(c) The Office of Counterintelligence may conduct an in-depth interview with the individual, may request relevant information from the individual, and may provide an opportunity for the individual to undergo an additional polygraph examination.

(d) Whenever information is developed by the Office of Security indicating counterintelligence issues, the Director of the Office of Security shall notify the Director of the Office of Counterintelligence.

(e) If, in carrying out a comprehensive CI evaluation of an individual under this section, there are significant unresolved issues, not exclusively related to polygraph examination results, indicating counterintelligence issues, then the Director of the Office of Counterintelligence shall notify the DOE national laboratory director (if applicable), plant manager (if applicable) and program manager(s) for whom the individual works that the individual is undergoing a CI evaluation pursuant to this part and that the evaluation is not yet complete.

§ 709.16 Application of Counterintelligence Evaluation Review Boards in reaching conclusions regarding CI evaluations.

(a) *General.* If the results of a counterintelligence evaluation are not dispositive, the Director of the Office of Counterintelligence may convene a Counterintelligence Evaluation Review Board to obtain the individual views of each member as assistance in resolving counterintelligence issues identified during a counterintelligence evaluation.

(b) *Composition.* A Counterintelligence Evaluation Review Board is chaired by the Director of the Office of Counterintelligence (or his/her designee) and includes representation from the appropriate line Program Managers, lab/site/facility management (if a contractor employee is involved), the DOE Senior Intelligence Officer, the DOE Office of Security and security directors for the DOE or NNSA site or operations office.

(c) When making a final recommendation under § 709.17 of this part, to a program manager, the Director of Counterintelligence shall report on the Counterintelligence Evaluation Review Board's views, including any consensus recommendation, or if the members are divided, a summary of majority and dissenting views.

§ 709.17 Final disposition of CI evaluation findings and recommendations.

(a) Following completion of a CI evaluation, the Director of the Office of Counterintelligence must recommend, in writing, to the appropriate Program Manager that the individual's access be approved or retained, or denied or revoked.

(b) If the Program Manager agrees with the recommendation, the Program Manager will notify the individual that the individual's access has been approved or retained, or denied or revoked.

(c) If the Program Manager disagrees with recommendation of the Director of the Office of Counterintelligence, the matter is referred to the Secretary for a final decision.

(d) If the Program Manager denies or revokes the individual's access, and the individual is a DOE employee, DOE may reassign the individual or realign the individual's duties within the local commuting area or take other actions consistent with the denial of access.

(e) If the Program Manager revokes the access of an individual detailed to DOE, DOE may remove the individual from access to the information that justified the CI evaluation and return the individual to the agency of origin.

(f) For cases involving a question of loyalty to the United States, the Director of the Office of Counterintelligence may refer the matter to the FBI as required by section 145d of the AEA. For cases indicating that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, DOE is required by 50 U.S.C. 402a(e) to refer the matter to the Federal Bureau of Investigation.

(g) Utilizing the DOE security criteria for granting or denying an access authorization under 10 CFR part 710, the Office of Counterintelligence makes a determination whether an individual completing a CI evaluation has made disclosures that warrant referral, as appropriate, to the Office of Security or the Manager of the applicable DOE/NNSA Site, Operations Office or Service Center. The Office of Counterintelligence does not report minor security infractions that do not create a serious question as to the individual's eligibility for a personnel security clearance.

Subpart C—Safeguarding Privacy and Employee Rights

§ 709.21 Requirements for notification of a polygraph examination.

When a polygraph examination is scheduled, the DOE must notify the individual, in writing, of the date, time, and place of the polygraph examination, the provisions for a medical waiver, and the individual's right to obtain and consult with legal counsel or to secure another representative prior to the examination. DOE must provide a copy of this part to the individual. The individual must receive the notification at least ten days, excluding weekend days and holidays, before the time of the examination except when good cause is shown or when the individual waives the advance notice provision.

§ 709.22 Individual rights to counsel or other representation.

(a) At the individual's own expense, an individual has the right to obtain and consult with legal counsel or another representative. The counsel or representative may not be present during the polygraph examination. Except for interpreters and signers, no one other than the individual and the examiner may be present in the examination room during the polygraph examination.

(b) At the individual's own expense, an individual has the right to obtain and consult with legal counsel or another representative at any time during an interview conducted in accordance with § 709.15 of this part.

§ 709.23 Obtaining individual consent to a polygraph examination.

DOE may not administer a polygraph examination unless DOE:

(a) Notifies the individual of the polygraph examination in writing in accordance with § 709.21of this part; and

(b) Obtains written consent from the individual prior to the polygraph examination.

§ 709.24 Other information provided to the individual prior to a polygraph examination.

Before administering the polygraph examination, the examiner must:

(a) Inform the individual of the use of audio and video recording devices and other observation devices, such as two-way mirrors and observation rooms;

(b) Explain to the individual the characteristics and nature of the polygraph instrument and examination;

(c) Explain the physical operation of the instrument and the procedures to be followed during the examination;

(d) Review with the individual the relevant questions to be asked during the examination;

(e) Advise the individual of the individual's privilege against self-incrimination; and

(f) Provide the individual with a pre-addressed envelope addressed to the Director of the Office of Counterintelligence in Washington, DC, which may be used to submit a quality assurance questionnaire, comments or complaints concerning the examination.

§ 709.25 Limits on use of polygraph examination results that reflect ''Significant Response'' or ''No Opinion''.

DOE or its contractors may not:

(a) Take an adverse personnel action against an individual or make an adverse access recommendation solely on the basis of a polygraph examination result of ''significant response'' or ''no opinion''; or

(b) Use a polygraph examination that reflects ''significant response'' or ''no opinion'' as a substitute for any other required investigation.

§ 709.26 Protection of confidentiality of CI evaluation records to include polygraph examination records and other pertinent documentation.

(a) DOE owns all CI evaluation records, including polygraph examination records and reports and other evaluation documentation.

(b) Except as provided in paragraph (c) of this section, the Office of Counterintelligence maintains all CI evaluation records to include polygraph examination records and other pertinent documentation acquired in conjunction with a counterintelligence evaluation in a system of records established under the Privacy Act of 1974 (5 U.S.C. 552a).

(c) The Office of Intelligence also may maintain polygraph examination reports generated with respect to individuals identified under § 709.3(a)(2) in a system of records established under the Privacy Act of 1974.

(d) DOE must afford the full privacy protection provided by law to information regarding an employee's refusal to participate in a CI evaluation to include a polygraph examination and the completion of other pertinent documentation.

(e) With the exception of the polygraph report, all other polygraph examination records are destroyed ninety days after the CI evaluation is completed, provided that a favorable recommendation has been made to grant or continue the access to the position. If a recommendation is made to deny or revoke access to the information or involvement in the activities that justified conducting the CI evaluation, then all the records are retained at least until the final resolution of any request for reconsideration by the individual or the completion of any ongoing investigation.

Subpart D—Polygraph Examination and Examiner Standards

§ 709.31 DOE standards for polygraph examiners and polygraph examinations.

(a) DOE adheres to the procedures and standards established by the Department of Defense Polygraph Institute (DODPI). DOE administers only DODPI approved testing formats.

(b) A polygraph examiner may administer no more than five polygraph examinations in any twenty-four hour period. This does not include those instances in which an individual voluntarily terminates an examination prior to the actual testing phase.

(c) The polygraph examiner must be certified to conduct polygraph examinations under this part by the DOE Psychophysiological Detection of Deception/Polygraph Program Quality Control Official.

(d) To be certified under paragraph (c) of this section, an examiner must have the following minimum qualifications:

(1) The examiner must be an experienced CI or criminal investigator with extensive additional training in using computerized instrumentation in Psychophysiological Detection of Deception and in psychology, physiology, interviewing, and interrogation.

(2) The examiner must have a favorably adjudicated single-scope background investigation, complete a CI-scope polygraph examination, and must hold a ''Q'' access authorization, which is necessary for access to Secret Restricted Data and Top Secret National Security Information. In addition, he or she must have been granted SCI access approval.

(3) The examiner must receive basic Forensic Psychophysiological Detection of Deception training from the DODPI.

§ 709.32 Training requirements for polygraph examiners.

(a) Examiners must complete an initial training course of thirteen weeks, or longer, in conformance with the procedures and standards established by DODPI.

(b) Examiners must undergo annual continuing education for a minimum of forty hours training within the discipline of Forensic Psychophysiological Detection of Deception.

(c) The following organizations provide acceptable curricula to meet the training requirement of paragraph (b) of this section:

(1) American Polygraph Association;

(2) American Association of Police Polygraphists; and

(3) Department of Defense Polygraph Institute.

PART 710—CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SPECIAL NUCLEAR MATERIAL

2. The authority citation for part 710 is revised to read as follows:

Authority: 42 U.S.C. 2165, 2201, 5815, 7101, *et seq.*; 7383h–1; 50 U.S.C. 2401, *et seq.;* E.O. 10450, 3 CFR 1949–1953 Comp. p. 936, *as amended;* E.O. 10865, 3 CFR 1959–1963 Comp. 398, *as amended.*

3. Section 710.6 is amended by redesignating paragraph (a) as paragraph (a)(1) and by adding a new paragraph (a)(2) which reads as follows:

§ 710.6 Cooperation by the individual.

(a) * * *

(2) It is the responsibility of an individual subject to 10 CFR 709.3(c) to consent to and take an event-specific polygraph examination. A refusal to consent to or take such an examination may prevent DOE from reaching an affirmative finding required for continuing access authorization. In this event, DOE may suspend or terminate any access authorization.

* * * * *

[FR Doc. 05–248 Filed 1–6–05; 8:45 am]

BILLING CODE 6450–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 71

[Docket No. FAA–2004–19813; Airspace Docket No. 04–AAL–26]

Proposed Revision of Class E Airspace; Point Lay, AK

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed rulemaking.

SUMMARY: This action proposes to revise the Class E airspace at Point Lay, AK. Three new Standard instrument approach procedures (SIAP's) are being published for Point Lay, AK. Additional Class E airspace is needed to contain aircraft executing instrument approaches at Point Lay Airport. Adoption of this proposal would result in additional Class E airspace upward from 1,200 feet (ft.) above the surface at Point Lay, AK.

DATES: Comments must be received on or before February 22, 2005.

ADDRESSES: Send comments on the proposal to the Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590–0001. You must identify the docket number FAA–2004–19813/ Airspace Docket No. 04–AAL–26, at the beginning of your comments. You may also submit comments on the Internet at *http://dms.dot.gov.* You may review the public docket containing the proposal, any comments received, and any final disposition in person in the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Docket Office (telephone 1–800–647–5527) is on the plaza level of the Department of Transportation NASSIF Building at the above address.

An informal docket may also be examined during normal business hours at the office of the Manager, Safety, Alaska Flight Services Operations, Federal Aviation Administration, 222 West 7th Avenue, Box 14, Anchorage, AK 99513–7587.

FOR FURTHER INFORMATION CONTACT: Jesse Patterson, AAL–538G, Federal Aviation Administration, 222 West 7th Avenue, Box 14, Anchorage, AK 99513–7587; telephone number (907) 271–5898; fax: (907) 271–2850; e-mail: *Jesse.CTR.Patterson@faa.gov.* Internet address: *http://www.alaska.faa.gov/at.*

SUPPLEMENTARY INFORMATION:

Comments Invited

Interested parties are invited to participate in this proposed rulemaking by submitting such written data, views, or arguments as they may desire. Comments that provide the factual basis supporting the views and suggestions presented are particularly helpful in developing reasoned regulatory decisions on the proposal. Comments are specifically invited on the overall regulatory, aeronautical, economic, environmental, and energy-related aspects of the proposal. Communications should identify both docket numbers and be submitted in triplicate to the address listed above. Commenters wishing the FAA to acknowledge receipt of their comments on this notice must submit with those comments a self-addressed, stamped postcard on which the following statement is made: ''Comments to Docket No. FAA–2004–19813/Airspace Docket No. 04–AAL–26.'' The postcard will be date/time stamped and returned to the commenter.

All communications received on or before the specified closing date for comments will be considered before taking action on the proposed rule. The proposal contained in this notice may be changed in light of comments received. All comments submitted will be available for examination in the