

Oversight - Department of Energy polygraph program
Full Committee Hearing
The Honorable Kyle E. McSlarrow
Deputy Secretary of Energy , Department of Energy

Thank you for giving me the opportunity to appear before you today to discuss the Department of Energy's current efforts and intentions regarding a new polygraph examination policy. This testimony is specific to the DOE polygraph program as it is administered by the DOE. The DOE utilizes a format that differs from the format used by some other Federal agencies. My statements today should therefore not be construed as offering any opinion on any other polygraph program in the Federal government.

I. Introduction

Let me start by providing some historical perspective on this matter. Both the Executive and Legislative branches of our government have long recognized that the Department's national weapons laboratories are among the world's premier scientific research and development institutions. They are essential to our continued national security. They played a vital role in our victory in the Cold War, and they have continued to play a vital role in protecting the United States to this day. For that very reason, because they are the repository of America's most advanced know-how in nuclear and related weapons and the home of some of America's finest scientific minds and engineering capabilities, they also have been and will continue to be major targets of foreign intelligence services and other enemies of the United States. That has been true since they were created and it is equally true today.

In particular, the attractiveness of DOE's laboratories as an intelligence target has not abated as a result of the end of the Cold War. Rather, as this Committee is well aware, the number of nations possessing, developing, or seeking weapons of mass destruction continues to grow, as does the threat presented to American interests by rogue nations and terrorist groups seeking access to these materials. As a result, throughout our history, the Department of Energy, 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 this cutting edge scientific work, 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 the Department of Energy 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 to the matter before you today. 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 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, the Department of Energy proposed a rule, entitled "Polygraph Examination Regulation," that would govern the use of the polygraph as a screening tool. It proposed that all 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 National Defense Authorization Act for FY2000, Congress endorsed the approach by directing 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 National Defense Authorization Act 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 National Defense Authorization Act for FY2002 (PL 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. Finally, Congress provided that the requirements it had imposed in the two earlier Defense Authorization Acts regarding the DOE Counterintelligence Polygraph Program would be repealed upon certification by the Secretary to the Congressional Defense Committees that DOE has promulgated and fully implemented a new polygraph rule. We understand this to mean that the Department is not constrained by those requirements in developing the rule it may elect to promulgate.

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. 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.

The Secretary then directed me 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 my review. I have worked closely with the Administrator of the National Nuclear Security Administration and the three directors of the nuclear weapons labs. I have discussed these issues with counterintelligence professionals, polygraph experts, and, as part of that review, I have 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. II. Basis for Recommendations

I have recently completed that review process. Let me say up front that this is one of the most difficult public policy issues I have had to confront. There is something almost talismanic about polygraphs. I can personally attest to this, since both the Secretary and I took a polygraph exam early in our tenure at the Department. I will discuss specific NAS recommendations throughout my testimony, but 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. I found many of the NAS’s concerns about the “validity” of polygraph testing to be well taken. I have personally discussed this issue with many employees, some of whom 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, as a policy maker, I have concluded 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 other observers.

I am therefore recommending to the Secretary that we propose substantial changes to how we use the polygraph in the context of the Department’s counterintelligence program. In doing so, I carefully weighed considerations of fairness to employees with national security objectives. I 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. I 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. I 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. Throughout, I was 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.

Because I have recommended that we propose substantial changes that encompass the classes of individuals who would be subject to a counterintelligence scope polygraph exam and the

procedures that apply to the use of polygraphs, if the Secretary accepts my recommendation we will also publish a new proposed rule. Such a proposal will entail significant consultation within the executive branch. I would anticipate such a proposed rule would be published by the end of this year. In addition to public comment, I would expect the Department to hold a public hearing before finalizing the rule.

I would like now to summarize the changes that I am recommending to the current polygraph program. As I do so, I will identify the considerations I concluded were most important taking into account the NAS report.

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 the Department's program, 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 produced positive results.

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 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. I will not detail it fully here. However, the bottom line is that I 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 my response is twofold. First, I believe 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. As I will note below, that has led me to recommend that we substantially lower the numbers of categories of information and hence the numbers of persons that would be subject to a polygraph screen.

Even in such cases, however, I still believe 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. We cannot afford them because they risk undermining the very national security goals we hope to attain. That brings me to the second element of my response. The NAS paragraph quoted above actually only goes to the use of the polygraph results as the sole basis for decision-making. 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 me to be far less problematic because we 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: I know of no kind of investigative lead that is perfect. Most will identify a substantial number of instances of misconduct or “false positives” that do not check out. Let us take anonymous tips, which 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 on account 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 decision-making.

Similarly, techniques in addition to the polygraph are utilized by U.S. Government agencies, including DOE, 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 of neighbors, co-workers and others. 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 to my knowledge 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. It seems to me that 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, I believe we should continue to use the polygraph as one tool to assist in making that determination, but that we not use it as the only tool. That, in turn, leads me to believe that we make clear not only, as we do now in our current rule, that we will not take any “adverse personnel action” solely based on the test results of polygraph examinations, but that it is also our 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 that we intend that a polygraph screen serve what we have previously said it would: that is, a “trigger” that may often be useful for subsequent investigation, but standing

alone treated as having no conclusive evidentiary value. In every case of an adverse personnel action, it would be our policy that such an action or decision would be based on other information as well.

Let me now turn to 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. My review of this question persuades me 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 the Department’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.

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 don’t “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.

Thus, in making my recommendations, I intend to give greater scrutiny to those concerns the NAS Report identified. In particular, as a result of the NAS Report, I have already directed a review of our current practice under the Accelerated Access Authorization Program, where interim clearances are granted for some personnel, based in part on whether they “pass” a polygraph exam, even before the completion of a background check (Other requirements for interim clearance under this program include completion of Questionnaire for National Security Positions, a National Agency Check with Credit, psychological screening and drug testing). I also believe it is critical that everyone at DOE involved in access determinations – Counterintelligence, Security, and Program personnel -- truly internalize the NAS’s points on both “false positives” and “false negatives” and build them into the culture of their organizations, particularly the people charged with making access recommendations or decisions. III. Overview of Recommended Changes

I am recommending 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.

My recommendation is to retain a mandatory polygraph screening program only for individuals with regular access to the most sensitive information. I recommend that the proposed rule, like the current regulation, provide for a mandatory counterintelligence scope polygraph examination

prior to initial access being granted, as well as periodic polygraph examinations at intervals not to exceed five years.

Overall, my recommendation is to narrow the range of information, access to which will trigger mandatory screening as compared to the potential scope of the program under the current rule. The approach I am recommending would have the effect of reducing the number of individuals affected from well in excess of potentially 20,000 under the current rule to approximately 4,500 under this new program.

I will recommend that some elements of the mandatory screening population remain essentially the same as under the current regulation. For example: all counterintelligence positions; all positions in the Headquarters Office of Intelligence and at the Field Intelligence Elements; and all positions 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 positions would continue to be subject to mandatory screening because they involve routine access to highly sensitive information, such as foreign intelligence information and other extremely close-hold and compartmented information.

In my own thinking about the justifications for use of the counterintelligence scope polygraph, I have searched for a test to identify the types of information that on balance overcame 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 to me 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”.

Another consideration is that even equally critical information may be targeted differently. In some cases, such information may reside in seemingly innocuous offices anywhere in the country. In the case of the Department, no such possibility exists. All of our facilities, and certainly the three weapons labs, are well known to involve the most sensitive secrets our country possesses, not simply about nuclear weapons, but about countless other programs. Therefore, there can be no question that these facilities will be targeted by those who wish to do us harm. Thus, we would propose including in the mandatory screening program those positions with routine or continuing access to all DOE-originated Top Secret information, including Top Secret Restricted Data and Top Secret National Security Information. 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.

Let me make clear that this category will not include everyone with a “Q” or a Top Secret clearance, nor will it include all weapons scientists; it will include only those whose positions require continuing, routine access to Top Secret RD or other DOE-originated Top Secret information. This is a fairly small population, probably less than one thousand people complex-wide.

I am also making a separate recommendation regarding certain DOE-originated information. We possess certain nuclear weapons information – referred to as “Sigma” information – classified at a

level below Top Secret that deals with various sensitive aspects of the nuclear weapons program to which we formally restrict access, including vulnerability information (Sigma 14), use control information (Sigma 15), and other design information (Sigmas 1 and 2). This information would be particularly attractive to terrorist organizations because it could facilitate the deliberate unauthorized use (nuclear detonation) of a nuclear weapon or the construction of an Improvised Nuclear Device. I am recommending to the Secretary that he direct a review to determine whether, as a result of our understanding of current threats and other factors, some or all of this "Sigma" information should be reclassified at the Top Secret level or protected under a Special Access Program. The conclusions of this review could result in additional positions in this category.

I will also recommend to the Secretary that the new proposed rule include authority for certain managers, with input from the Office of Counterintelligence and subject to the approval of either the Secretary or the Administrator of the National Nuclear Security Administration, to include additional individuals within their offices or programs in the mandatory screening program. These individuals will be limited to those with regular access to information or other materials presenting the highest risk. 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, the Personnel Assurance Program, and the Personnel Security Assurance Program.

I intend to recommend that we no longer designate for mandatory polygraph screening all individuals in the Personnel Assurance Program and the Personnel Security Assurance Program (which, as an aside, we are in the process of combining into a single Human Reliability Program with uniform clearance requirements). The FY 2000 NDAA originally mandated that everyone in these programs be subject to a screening polygraph, and the FY 2001 NDAA retained that mandate. Accordingly, the current regulation likewise mandates that they all be screened. The FY 2002 NDAA, however, directs that the focus of DOE's polygraph program be the protection of classified data, materials or information. The PAP and PSAP programs apply to individuals not by reason of their access to classified information but on account of their responsibilities for nuclear materials. Many, if not most, of the individuals in positions associated with these programs do not have routine access to the most sensitive classified information, leading me to recommend against their wholesale inclusion in the mandatory screening program.

Before I leave the mandatory screening program, let me mention that if a revised rule is proposed and promulgated, I believe it is important that we proceed with full implementation of that rule expeditiously so that the Secretary is in a position to make the certification required by the FY 2002 NDAA regarding implementation of the new program. I would envision, as one element of the new program, we would allow incumbents in positions designated for mandatory screening under the new regulation to retain access to their programs pending scheduling of their first polygraph examination.

Let me now address an entirely new proposed element of the overall program – the random screening program. We have identified a universe of positions whose level and frequency of access, while not requiring mandatory screening, nevertheless warrants some additional measure of deterrence against damaging disclosures.

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 me as too simplistic. The types of information we are concerned with don't 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 that I identified above 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 the Department command the full attention of the Department’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, I believe that 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 me 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 specific programs or positions 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, polygraph examinations 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 polygraph examinations at any time, at any frequency. In essence, even though it is possible that an individual in such a position may never actually be selected through the random process, the individual could be subject to a (random) polygraph 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 our policy to fashion a random polygraph program that achieves the objectives of deterrence with the minimum reasonable percentage or number of individuals in those positions to which it applies. Since we estimate the total number of individuals who would be eligible for the random polygraph program to be about 6000, the use of a minimum percentage means the total number of random polygraphs in any given year would be a much lower number.

The following positions would be included in the random screening program: all positions in the offices of Security, Emergency Operations, and Independent Oversight and Performance Assurance that are not designated for the mandatory screening program; positions with routine access to Sigma 14 and 15 weapons data; and system administrators for classified cyber systems. Again, the population associated with routine access to Sigma 14 and 15 weapons information

will not encompass the entire population of “Q” cleared individuals, but only those with regular access to Sigma 14 and 15 information.

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. We intend to evaluate the merits of including system administrators of unclassified cyber systems in the random program at a later date.

In addition to the mandatory and random screening programs, I intend to recommend that we clarify in the regulation that the Department may also conduct “specific-incident” polygraph examinations in response to specific facts or circumstances with potential counterintelligence implications. 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 rule will also retain provisions for voluntary polygraphs such as exculpatory polygraph examinations conducted in response to questions that have arisen in the context of counterintelligence investigations or personnel security issues.

As I made clear in the discussion above, 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 polygraph examinations. Therefore I will recommend that the new proposed rule retain and enhance the protections already contained in the current regulation. The provisions we would retain include: written notification by the Department and written consent from the employee are required before a polygraph examination can be administered; DOE is prohibited from recording a refusal to submit to a polygraph examination in an employee’s personnel file; audio and video recordings of polygraph examination sessions are made to protect both the employee and the polygrapher; all polygraph examination records and reports are maintained in a system of records established under the Privacy Act; and strict qualification standards and standards of conduct for polygraphers are established and enforced. Neither the polygrapher nor the Office of Counterintelligence has the authority to make a decision to grant or deny access. That decision is made by the Program Manager or the Secretary. The 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. The examiner may not ask questions that concern conduct that has no counterintelligence implication or concern conduct that has no direct relevance to an investigation, such as “lifestyle” questions.

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 specific-incident investigations 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 as I recommend we do is the most important step I believe we can take to limit these kinds of problems. In addition, however, I believe we can make a few improvements to the current rule. First, I believe we should 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, we do 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. Therefore, somewhat curiously, the current prohibition on an "adverse personnel action" solely based on polygraph results prohibits a use of the polygraph not really contemplated by the rule in the first place.

Accordingly, I recommend that we also make clear that it is our policy not to base a denial of access solely on the results of a polygraph exam. 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."

I am also recommending that the new regulation 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 that may be convened to consider the results of counterintelligence evaluations that are not dispositive. I also recommend that it be our policy that the appropriate weapons laboratory director be consulted when the access determination involves a laboratory employee. I also believe we need to place a premium on thorough but speedy decision-making on these issues, which I believe is in the best interest of both the employee and the Department. I am also recommending that we consider establishing a separate mechanism, within the Department but external to the Office of Counterintelligence, to evaluate any complaints lodged against polygraphers and identify and correct specific issues associated with the conduct, performance, or training of polygraphers.

Finally, as I mentioned previously, I am recommending that we commit to review, not later than two years following the effective date of the regulation, the scope of the mandatory and random screening programs and the experience gained through the implementation of the regulation. The purpose of the review would be to consider whether any amendments to the regulation related to the process or to the covered population are appropriate.

Because the policy choices discussed above lead to the conclusion that the polygraph should be just one tool of many, I am recommending that we make clear in the new regulation that polygraphs are just one element to be used in broader counterintelligence evaluations resulting from polygraph examinations or other information. The current rule refers to review of personnel security files and personal interviews as elements of such evaluations. I am also recommending that we consider broadening this reference to note that these evaluations may also, in appropriate circumstances and to the extent authorized by law, use other techniques, such as reviews of medical and psychological examinations, analyses of foreign travel and foreign contacts and connections, examination of financial and credit information, and net worth analyses. We intend to consult closely with others in the executive branch regarding this potential aspect of our proposal.

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. In any event, we stand ready to lead or assist in such research.

That concludes my prepared statement. I will be happy to respond to any questions you have regarding our intentions for the proposed regulation on counterintelligence evaluations.

**Oversight - Department of Energy polygraph program
Full Committee Hearing**

**Dr. Stephen E. Fienberg , Chairman , National Research Council Committee to Review the
Scientific Evidence on the Polygraph**

Mr. Chairman, and Senators. I am pleased to appear before you this morning. I am Maurice Falk University Professor of Statistics and Social Science, in the Department of Statistics, the Center for Automated Learning and Discovery, and the Center for Computer and Communications Security, all at Carnegie Mellon University. I also served as the Chair of the National Research Council's Committee to Review the Scientific Evidence on the Polygraph. Accompanying me today is Dr. Paul Stern, who served as the Study Director for the committee. The committee's report, *The Polygraph and Lie Detection*, which was released last October reviewed the scientific evidence underlying the use polygraphs for security screening of employees at the national laboratories. It also considered the potential alternatives to polygraph testing for the detection of deception. My testimony today is based on that report.

The NAS-NRC Committee Report

The committee's report begins by setting the current debate over the efficacy of polygraph testing in the context of the mystique that surrounds it—this includes a culturally shared belief that the polygraph is nearly infallible. As we note in the report, the scientific evidence strongly contradicts this belief.

Let me now briefly summarize the committee's principal conclusions:

1. The scientific evidence supporting the accuracy of the polygraph to detect deception is intrinsically susceptible to producing erroneous results.
2. In populations of naïve examinees untrained in countermeasures, specific incidence polygraph tests can discriminate lying from truth telling at rates well above chance, though well below perfection. But the accuracy of the polygraph in screening situations is almost certainly lower.
3. Basic science gives reason for concern that polygraph test accuracy can be degraded by countermeasures.
4. The scientific foundations of polygraph screening for national security were weak at best and is insufficient to justify reliance on its use in employee security screening in federal agencies.
5. Some potential alternatives to the polygraph show promise, but none has been shown to outperform the polygraph and none is likely to replace it in the short term.

I have appended the Executive Summary of the report to this testimony as it contains the specific wording of these conclusions and details explaining how the committee reached them.

The DOE Proposed Regulations

In April of this year, the Department of Energy released new draft regulations on its program of polygraph testing of eight classes of federal employees and contractors who have access to

classified information. The new regulations would continue a policy that was set in place in 2000 but suspended in 2001, pending the report of the NAS-NRC committee. Thus it might be natural to ask what in the report is of direct relevance to the proposed regulations.

Let me return to the specific wording of the committee's recommendation on the matter of security screening:

Polygraph testing yields an unacceptable choice for DOE employee security screening between too many loyal employees falsely judged deceptive and too many major security threats left undetected. 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.

How does DOE square these conclusions with its plan to continue the polygraph policy unchanged? It says that the polygraph, though "far from perfect, will help identify some individuals who should not be given access to classified data, materials, or information." This may be true, but two other things about polygraph screening are also true that should give pause.

First, for every such individual identified, hundreds of loyal employees will be misidentified as possible security threats. Our report make clear that, given DOE's own expected rates of security violations, someone who "fails" the DOE polygraph screening test has over a 99 percent chance of actually being a truthful person. Unfortunately, the DOE doesn't have any other scientific tool to fall back on to distinguish the security violators from the innocent people falsely accused.

Second, any spy or terrorist who takes the DOE's polygraph test is far more likely to "pass" the test than to "fail" it—even without doing anything to try to "beat" the test. Efforts at so-called countermeasures are likely to increase further the chances that a committed spy or terrorist will "beat" the test. This is the most serious problem with polygraph screening, especially in these times of terrorist threat: the possibility that security officials will take a "passed" polygraph too seriously, and relax their vigilance.

The DOE regulations give every indication that the agency has just this sort of overconfidence in polygraph tests that give "passing" results. The proposed regulations say, "DOE's priority should be on deterrence and detection of potential security risks with a secondary priority of mitigating the consequences of false positives and false negatives." The committee found little scientific evidence to support the effectiveness of the polygraph in this regard. Moreover, it concluded that the consequences of false negative tests—tests that deceivers "pass"—should have top priority, because it is those test results that leave the nation open to the most serious threat, from people whose continued access to sensitive information is justified because they "passed the polygraph."

The DOE, in continuing to rely on polygraph screening just as before, is doing more for the appearance of security than for the reality. Moreover, while some potential alternatives to polygraphs show promise, none has led to scientific breakthroughs in lie detection. Thus we cannot look for a short-term quick technological fix to aid us in our quest for securing the nation and its secrets.

The nuclear weapons labs need a strong security program, not a false sense of security. There are better alternatives than maintaining the previous polygraph policy. Last year, the DOE's Commission on Science and Security recommended management and technological changes at the labs that could make unauthorized release of national secrets more difficult to conduct and easier to detect without relying on the polygraph or other methods of employee screening—all of

which are seriously limited and have little or no scientific base. There may still be a place for polygraph testing in the labs, for investigations and for a small number of individuals with access to the most highly sensitive classified information, if the test's limited accuracy is fully acknowledged. But broad use of this flawed test for screening will probably do more harm than good. National security is too important to be left to such a blunt instrument.

Conclusion

Let me conclude by reminding you that polygraph testing now rests on weak scientific underpinnings despite nearly a century of study. And much of the available evidence for judging its validity lacks scientific rigor. Our committee sifted the existing evidence and our report made clear the polygraph's serious limitations in employee security screening. Searching for security risks using the polygraph is not simply like search for a needle in a haystack. It is true that, of the large groups of people being checked, only a tiny percentage of individuals examined are guilty of the targeted offenses. Unfortunately tests that are sensitive enough to spot most violators will also mistakenly mark large numbers of innocent test takers as guilty. Further, tests that produce few of these types of errors, such as those currently used by the DOE, will not catch most major security violators—and still will incorrectly flag truthful people as deceptive. Thus the haystack analogy fails to recognize the unacceptable trade-off posed by these two types of errors.

Our committee concluded that the government agencies could not justify their reliance on the polygraph for security screening. The proposed DOE regulations appear to disregard our findings and conclusions. As a nation, we should not allow ourselves to continue to be blinded by the aura of the polygraph. We can and should do better.

I would be happy to answer your questions and amplify on these comments.