STATEMENT OF GREGORY H. FRIEDMAN

INSPECTOR GENERAL

DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY,
VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS
OF THE
COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

FOR RELEASE ON DELIVERY
EXPECTED AT
9:00 AM

Thursday, March 15, 2001

Good morning Mr. Chairman and members of the Subcommittee. I am pleased to be here to respond to your request to testify on the major performance and management challenges confronting the Department of Energy (Department).

Recently, the Office of Inspector General (OIG) issued a special report on *Management Challenges at the Department of Energy* (DOE/IG-0491, November 2000). In that report, we categorized the most serious challenges facing the Department as follows:

- Startup of the National Nuclear Security Administration (NNSA)
- Contract Administration
- Energy Supply/Demand Technology
- Environmental Remediation
- Human Capital
- Information Technology
- Infrastructure
- Property Controls and Asset Inventories
- Safety and Health
- Security

Our analysis focused on those challenges that, in our view, warranted increased emphasis or appeared to have reached a heightened level of urgency. Many of our observations concerned issues related to the Department's national security and nuclear missions and may, therefore, be of particular interest to the Subcommittee.

Progress in resolving these issues will, in part, be impacted by the Department's effective implementation of the Government Performance and Results Act (Results Act). The Results Act requires an agency to develop goals, measures, and metrics to clearly establish what its intended outcomes are, what means it will use to achieve them, and

how it will know if it has been successful. The need to improve the Department's performance through better implementation of the Results Act has been a consistent theme of the work of my office. For example, in each of our last three annual reports on the Department's consolidated financial statements we have been critical of performance measures that were not meaningful or relevant, not quantifiable, and not clearly stated.

With regard to the overall management challenges, I am pleased to report that Secretary Abraham has asked that my office provide him with a full briefing on the challenge areas once his senior staff is in place. I will now briefly summarize our observations regarding the challenge areas.

Startup of the NNSA

NNSA was established in March 2000 pursuant to Title 32 of the National Defense Authorization Act for Fiscal Year 2000 (Public Law 106-65). NNSA is to provide clear and direct lines of accountability and has responsibility for the management and operation of the nation's nuclear:

- Weapons;
- Naval propulsion program; and
- Nonproliferation activities.

The NNSA faces a number of significant challenges. Logistical and organizational issues must be resolved; expectations, responsibilities, and authorities must be established; and, human capital issues must be addressed. In addition, many of the Department's longstanding challenge areas – notably contract administration, security, infrastructure, and information technology – now must be addressed by the NNSA as well.

Also, a number of major policy issues confront NNSA. One example is reducing the threat of nuclear proliferation and nuclear terrorism by helping to upgrade physical protection and material control and accounting systems at nuclear facilities in the states of the Former Soviet Union. Our audit on this subject, *Nuclear Material Protection, Control, and Accounting Program* (DOE/IG-0452, September 1999), disclosed that enhancements were needed to ensure that funds and equipment sent to these states were used for their intended purposes. We identified instances where low priority upgrades were funded and found that U.S. project teams lacked access to certain key facilities where upgrades were located.

Over the past several months, the OIG has worked to design a strategy for maximizing the effectiveness of our services relative to NNSA operations. General Gordon and I have met monthly since his appointment as Administrator of NNSA to discuss the unique challenges NNSA faces and ongoing OIG reviews of NNSA programs.

Contract Administration

In its Fiscal Year 2000 *Accountability Report*, the Department reported that most procurement challenges as defined by its Contract Reform effort have been resolved. Based on our observations and reviews, we have concluded that many of the Department's contract reform goals have yet to be achieved. For example, while incentives have been included in most Department contracts, OIG reviews have disclosed systemic weaknesses in the way these incentives have been administered. Further, while fees have, in fact, risen dramatically, OIG reviews have disclosed that there has not been a commensurate increase in financial risk or accountability of the Department's major contractors. In addition, performance measures have not been fully established to clarify expectations and monitor contractor performance.

In our judgment, improvement in contracting practices represents one of the greatest opportunities for enhancing the economy and efficiency of Departmental, including NNSA, operations. Of the Department's total budget of about $18 billion, over $13 billion is spent by its major contractors.

For the Department, an integral part of contract administration is project management. My office has issued many reports that have been critical of the Department's planning, justification, and management of its major projects. Cost overruns, schedule delays, and other management problems have plagued Department projects, including the $47 billion Tank Waste project at Hanford and the National Ignition Facility at Lawrence Livermore

National Laboratory, now projected to cost about $3.5 billion when completed. The Office of Management and Budget has included "improving the Department's program and contract management" as one of its 12 agency-specific priority management objectives for Fiscal Year 2001.

Energy Supply/Demand Technology

Another critical challenge facing the Department and the nation is assuring the adequate supply of affordable energy resources. In a 1997 report, the Energy Research and Development Panel of the President's Committee of Advisors on Science and Technology noted that the nation's economic well-being depends on reliable, affordable supplies of energy. The Panel further commented that "…our national security requires secure supplies of oil or alternatives to it…" and that, as a consequence, the United States must maintain its leadership in the science and technology of energy supply and use.

Last year's dramatic spike in oil prices led to a renewed national focus on the significance of oil imports and the technology that can mitigate energy dependency. Currently, the United States relies on petroleum for about 40 percent of its energy supply, and 51 percent of this petroleum is imported. Increasing energy demands for transportation, as well as for other sectors of our economy, are likely to exacerbate this situation. For example, the Department projects that U.S. oil imports will increase from 51 percent in 1999 to 64 percent in 2020.

In light of the implications for our economic and national security, the Department should, in our judgment, intensify its efforts in the following areas:

- Availability of competitively-priced oil and natural gas supplies;
- Efficiency and productivity of energy-intensive industries; and,
- Development and use of advanced transportation vehicles and alternative fuels.

Environmental Remediation

The Department's effort to address the environmental consequences of its nuclear weapons mission has been recognized as the largest remediation program of its kind ever undertaken. The Department is responsible for cleaning up 113 geographic sites located in 30 states and one territory. Sites range in size from as small as a football field to larger than the state of Rhode Island. Cleaning up the nuclear weapons legacy will take several decades and, according to the Department's most recent estimate, cost about $234 billion. This is the third largest liability on the nation’s balance sheet.

The Department has made some progress in defining the cleanup effort, estimating its scope, and prioritizing individual projects. However, OIG reviews have illustrated the need for increased management attention to achieving intended environmental cleanup outcomes. For example, our audit of *The Management of Tank Waste Remediation at the Hanford Site* (DOE/IG-0456, January 2000) showed that this $47 billion project did not have a completed baseline, critical path, or comprehensive project management plan

despite similar OIG findings dating to 1993. During another audit, *Decontamination and Decommissioning Contract at the East Tennessee Technology Park* (DOE/IG-0481, September 2000), we found that the decontamination of three buildings at that site was two years behind schedule and $94 million over budget.

The magnitude of the cleanup effort, along with its technical complexities and uncertainties, ensures that it will remain a Departmental challenge for the foreseeable future.

Human Capital

The Department has reported that since 1995, it has reduced Federal staff by over 25 percent through reductions in force, buyouts, and attrition during a hiring moratorium to meet lowered budget estimates. The staff eligible for retirement has increased from 6 percent to 11 percent in the last 5 years. By 2005, 34 percent of today's Federal staff will be eligible to retire.

The Department's major contractors have experienced similar losses. For example, at Lawrence Livermore National Laboratory, three times as many scientists left the laboratory in the first eight months of 2000 as in all of 1999. A senior Department official recently testified before Congress that in 10 years, most of our weapons designers with nuclear testing experience will have retired. Many of those retiring or resigning take with them technical and scientific knowledge that is not easily replaced. As just one

example, when the Department's newest warhead, the W88, reaches the end of its original design life in 2014, we may no longer have anyone with test-based job experience to help evaluate modifications that may be required.

The OIG has been monitoring this issue through our role in the Federal Managers' Financial Integrity Act process and other audit work. For example, in our report on *The U.S. Department of Energy's Efforts to Preserve the Knowledge Base Needed to Operate a Downsized Nuclear Weapons Complex* (DOE/IG-0428, October 1998), we recommended that the Department develop and implement a performance plan to preserve the nuclear weapons program knowledge base, including capturing information that could be provided only by retiring weapons experts. Although that recommendation remained open as of December 31, 2000, the Department reported to us that it has taken steps to "reinvigorate" its knowledge and records management and has developed a comprehensive approach to preserving the nuclear weapons program knowledge base. While it is evident that management recognizes the seriousness of its human capital problem, the Department needs to take aggressive action to ensure that it maintains the technical, scientific, and management resources it needs to meet its critical mission requirements.

Information Technology

The Clinger-Cohen Act required the Department to appoint a Chief Information Officer (CIO). The CIO is responsible for developing and implementing (1) an effective agency-

wide information technology capital investment strategy, (2) specific performance goals and measures, (3) monitoring of and reporting on information technology programs, and (4) integrated information technology architecture.

Since 1996, the OIG has issued ten audit reports identifying problems associated with the Department's implementation of the Clinger-Cohen Act and its management of an estimated $1.6 billion in annual information technology expenditures. Two of our most recent reports illustrate an ineffective investment strategy for information technology. In our audit of *Corporate and Stand-Alone Information Systems Development* (DOE/IG-0485, September 2000), we found that the Department had spent at least $38 million developing duplicative information systems. Duplicative systems existed or were under development at virtually all organizational levels within the Department. Similarly, during our audit of *Commercial Off-the-Shelf Software Acquisition Framework* (DOE/IG-0463, March, 2000), we found that the Department failed to take advantage of enterprise-wide software contracts that could have saved nearly $40 million on just one desktop software suite.

In addition to these information technology management issues, the OIG has also conducted extensive reviews regarding aspects of "cyber security." In recent years, the OIG has developed significant capability and expertise in identifying security weaknesses relating to information technology. Our Technology Audit Group and Technology Crimes Section are working together to coordinate these reviews. I will include these efforts in my discussion of security issues.

Infrastructure

For several years, the OIG has reported that the condition of the Department's infrastructure is inadequate and, in fact, is deteriorating at an alarming pace. This is particularly true of the nuclear weapons production infrastructure. We have concluded that the problem has become severe, requiring prompt management attention.

In its recently revised Strategic Plan, the Department identified key objectives for National Security, including the ability to (1) maintain and refurbish nuclear weapons; (2) achieve "robust and vital" scientific, engineering, and manufacturing capabilities; and, (3) ensure the "vitality and readiness" of the national nuclear security enterprise.

Based on our audit of the *Management of the Nuclear Weapons Production Infrastructure*, (DOE/IG-0484, September 2000), we found that some Stockpile Stewardship Plan milestones and goals have slipped, restoration costs have increased, and future nuclear weapons production work, as required by a Presidential Decision Directive, is at risk. Knowledgeable Department officials estimate that between $5 billion and $8 billion over current budgeted amounts will need to be invested to address the deteriorating infrastructure of the weapons production plants. The Department and NNSA must swiftly act to counter the effects of deferred maintenance on the production infrastructure and critical manufacturing capabilities.

Our audit of *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection* (DOE/IG-0483, September 2000) also demonstrated that the Department had not implemented its Critical Infrastructure Protection Plan. As a result, the Department faced increased risk of malicious damage to cyber-related critical infrastructure that could adversely impact its ability to protect critical assets and deliver essential services. We noted that the Department had not developed specific performance measures or goals to guide implementation of the Presidential Decision Directive.

Property Controls and Asset Inventories

For several years the OIG has been reporting that the Department has extensive inventories of nuclear and non-nuclear materials that may no longer be necessary due to mission changes. We have been concerned that funds spent to store and handle materials that are not needed could be put to better use and that potential safety and health concerns exist. The OIG also has reported significant deficiencies in controls over Government property.

In January 2000, as part of a larger cost-savings initiative, the Inspector General suggested that the Secretary initiate a Department-wide review to specifically identify excess or unneeded assets and schedule their safe disposal at the earliest possible time. Based in part on the OIG recommendation, the then Secretary announced, in March 2000,

a Departmental initiative to "clean out the attic" of unneeded, unused property. Since March, Department managers have been working to deploy a number of new processes, including on-line auctions, to deal with this issue. As of late 2000, the initiative was still ongoing.

While the Department deserves credit for its attention to this long-standing problem, recent OIG reviews raised new concerns about the adequacy of controls over property for which the Department has a continuing need or a stewardship responsibility. Our audit of *Non-Nuclear Weapons Parts at the Rocky Flats Environmental Technology Site* (DOE/IG-0475, June 2000) disclosed problems with the way Rocky Flats controlled, accounted for, and reported the value of its non-nuclear parts inventory. In our *Inspection of Surplus Computer Equipment Management at the Savannah River Site* (DOE/IG-0472, June 2000) we determined that a contractor did not comply with property management requirements for disposal of surplus computer equipment. Stored information, including Unclassified Controlled Nuclear Information, was not cleared from all surplus computers.

Safety and Health

Ensuring the safety and health of its workforce and the public is one of the Department's most difficult, long-term challenges. Safety and health issues encompass all activities relating to the identification, testing, handling, labeling, cleanup, storage, and/or disposal

of radioactive and hazardous waste. Other activities relate to nuclear safety and occupational and worker safety and health (e.g., nuclear safety standards).

As with the Environmental Remediation challenge, the OIG does not expect that the Department will resolve these complex issues in the near term. Rather, Department managers should take aggressive action to ensure that safety and health activities are carried out as efficiently and effectively as possible. Several recent OIG reviews showed that this was not always the case.

During our audit of the *Federal Energy Regulatory Commission's Dam Safety Program* (DOE/IG-0486, October 2000), for example, we concluded that, overall, the Commission conducted a thorough and comprehensive dam safety program. However, management inefficiencies led to a backlog of safety reports needing review. As a result, the Commission did not have complete, timely, and important information about the safety condition of some dams under its jurisdiction.

The OIG also received allegations of criminal misconduct regarding safety and health issues. For example, we received information that one of the Department's subcontractors was mixing hazardous materials with non-hazardous/non-regulated paint waste material. After an OIG investigation, the subcontractor was sentenced to three years probation and fined for the treatment of hazardous waste without a permit and for transportation of hazardous waste without a manifest.

A separate OIG investigation disclosed evidence that the president of a Department subcontractor authorized the submission of false bioassay data. The false test results may have inaccurately identified a person's actual exposure to nuclear materials, thus placing the person at risk. The Department took steps to retest employees affected by the false test results. Following a guilty plea for submitting false claims and false statements, the president of the company was sentenced to 3 months in a Bureau of Prisons halfway house, ordered to pay restitution and fines, and debarred from government contracting for 10 years.

Security

One of the Department's national security objectives is ensuring that the Department's "…nuclear weapons, materials, facilities, and information assets are secure through effective safeguards and security policy, implementation, and oversight." The Department spends over $1 billion per year for physical and personnel security. This includes NNSA and other Departmental sites. Previous reviews by the OIG, Congress, and others have identified weaknesses in the Department's protection of nuclear weapons-related information. Lapses in security were frequently cited during the debate leading to NNSA's creation.

Our Inspection report on *Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessment at Los Alamos National Laboratory* (DOE/IG-0471, May 2000), showed that certain security survey

ratings were changed without a documented rationale. This inspection also disclosed that about 30 percent of the Los Alamos security operations division personnel interviewed believed they had been pressured to change or mitigate security self-assessments. Another inspection addressed *Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process* (DOE/IG-0482, September 2000), where we identified significant problems in the manner in which site safeguards and security plans were reviewed and quality assurance issues were closed.

An *Inspection of the Sale of a Paragon Supercomputer by Sandia National Laboratories* (DOE/IG-0455, December 1999) determined that Sandia failed to exercise prudent management judgment in its decision to excess and sell a supercomputer to a Chinese national. The supercomputer was one of the world's 100 fastest computers and had been used by Sandia to support the Department's nuclear weapons testing program. As noted previously, our inspection dealing with computer equipment at the Savannah River Site in South Carolina (DOE/IG-0472) disclosed that management at that site did not assure that surplus computers were sanitized prior to disposal.

In our audit of *Unclassified Network Security at Selected Field Sites*, (DOE/OIG-0459, February 2000), the OIG identified significant weaknesses that increased the risk that unclassified computer networks could be damaged by malicious attack. Even though the Department became aware of a number of network security problems in recent years, it did not, until recently, issue specific network security requirements. Ongoing OIG work regarding the Department's Cyber Security Incident Response and Virus Reporting will

assess how well the Department is protecting its computer systems from damage by malicious software and intrusions.

Recent passage of the Government Information Security Reform Act, with its requirement for an annual independent evaluation of the Department's information security activities by the OIG, represents a significant additional challenge and a major demand on our staffing resources. We are developing a comprehensive strategy for meeting this new requirement in a manner that fully leverages our in-house capabilities, contractor resources, and the expertise of other information technology groups within the Department.

Areas of Progress

The Department has taken steps to address a number of previously reported problems. Specifically, Department managers have implemented OIG recommendations or otherwise improved processes related to:

- Integrating research and development activities;
- Commencing operations at the Waste Isolation Pilot Plant (WIPP);
- Improving financial reporting on environmental liabilities; and,
- Correcting the Year 2000 computer problem.

As this list illustrates, progress has been made in areas representing significant complexity. The improvements came about as a result of strategic planning and goal-setting, management commitment, and the concerted efforts of many Department and contractor personnel.

Conclusion

The Office of Inspector General looks forward to working with the Department's senior staff and with the Congress in a continuing effort to improve Department programs and operations.

Mr. Chairman, this concludes my statement and I would be pleased to answer any questions you may have.