June 20, 2002

Commission on Science and Security in the 21st Century DOE Accomplishments by Recommendation

1. Clarify Lines of Responsibility

   - Under Secretary Card's memorandum, "Principles for Office of Science Laboratory Contracts"- April 30, 2002, provides clarification of laboratory roles with respect to their authorities in contract execution.

   - Under Secretary Gordon's report to the Congress (February 25, 2002) provides guidance on the re-alignment of the NNSA organization structure designed to clarify roles and responsibilities related to line and staff functions at HQ and in the Field.

   - NNSA Policy Letter NAP-1; Establishment of a Policy Letter System for Managing Policy, Directives, and Business Practices within the NNSA. Formalizes NNSA roles and responsibilities relating to policy development.

   - DOE is implementing a PPBE system, building upon successful elements of the DoD system, but customized to meet NNSA's unique program and organizational requirements, which will aid in out year planning for science and security initiatives.

   - A separate complementary PPBE office has been created in the NNSA.

   - Under the new PPBE system, the statutorily required Five Year National Security Program (FYNSP) was completed in March 2002, endorsed by OMB, and provided to cognizant Congressional committees.

2. Integrate Science and Security

   - DOE and site contracting officials are in the process of incorporating ISSM policy language into site contacts, with reference to applicable DOE orders.

   - DOE and site contactors have conducted self-assessments against ISSM principles and functions, and are addressing gaps identified.

   - The Office of Security re-organized in November 2001 and now functions as a policy and support resource available to the program offices and facilities.

- The Office of Security in a May 31, 2002 memorandum urged the Program Secretarial Officers and the Laboratory Directors to fully participate in the security policy development quality panels as a further effort to ensure active science staff involvement in development of security policy.

- DOE is revising its award fee and civil penalties clauses to place the security program on similar footing with the safety program with respect to ensuring adequacy of incentives for effective security program performance.

- DOE Order 470.2A, Security and Emergency Management Independent Oversight and Performance Assurance Program, is being revised to reflect and clarify new OA roles and responsibilities and to address needed program improvements, particularly related to the corrective actions process following identification of security deficiencies by the oversight program.

- NNSA is changing the Operations Offices to service centers to streamline field program execution and remove an unnecessary layer of management oversight of the laboratories.

- The Office of Science is reviewing the applicability of service centers as part of the overall concept of reengineering.

3. Develop and Practice Risk-Based Security

- Draft Interim Design Basis Threat document was sent out for Departmental review in June 2002. The promulgation of the final Design Basis Threat will assist the Department in executing its risk management program.

- Issuance of a cost modeling tool/format, in November, 2001 and a new modeling tool, ATLAS, was issued for beta testing in June 2002 to provide additional rigor to the risk management process.

- Development of a revised DOE Order on the Unclassified Foreign Visit and Assignment (FV&A) completed in June 2002 to assist in flexible, prudent management of visitors to DOE facilities to provide necessary participation of foreign scientific expertise consistent with sound security practice.

- Preparation of revised "Zero Tolerance" policy completed in June 2002 to clarify expectations for protection of classified information while ensuring good judgment in identification of sanctions associated with mishandling of classified information.

- Preparation of a new Official Use Only (OUO) Information Order completed in June 2002 aimed at addressing the issue of "Sensitive, but Unclassified Information" through the establishment of three information types (classified, unclassified and Official Use Only).

- Office of Counterintelligence (CN) has taken numerous steps to increase its analytical capability within current resource limits aimed at improving the efficiency and timeliness of reviewing/analyzing sensitive and classified information:

    - Constructed and occupied a Sensitive Compartmental Information (SCI) Facility;
    - Extended the Intelligence Community SCI network into the facility;
    - Currently deploying a SECRET level, Wide Area Network to its field elements; and,
    - Refocused its assets on actionable/tactical analysis and support to countering terrorism.

- Establishment of Combating Terrorism Intelligence Working Group – Fall 2001, to enhance quality and timeliness of information sharing between relevant DOE offices.

4. Invest in New Tools and Techniques

- Roll-out of Public Key Infrastructure (PKI) for Federal employees (Entrust), initiated October 2001 to ensure ability to protect but manipulate sensitive information in an unclassified environment.

- Implemented a DOE Headquarters biometric (fingerprint) network login pilot program in October 2001 to improve efficiency of access control systems to sensitive/classified information areas.

- Introduction of Secure Compartmental Information (SCI) network connections to the Headquarters CN analysts to substantially enhance capabilities for timely acquisition and analysis of highly classified information.

- CN will have completed installation of a SECRET level network to CN field locations in August 2002 for improved efficiency in analysis of classified information in the field.

- Shifted additional Counterintelligence funding to Information Technology requirements efforts to accelerate improvements in cyber system architecture.

5. Strengthen Cyber Security

- DOE has in coordination and review the DOE Draft Order 476.x, to provide policy and guidance for continuous improvements of cyber security at DOE laboratories and across the DOE complex.

- The Chief Information Office (CIO) is developing a set of metrics that will be used to measure the effectiveness of current cyber security systems to aid in advancing overall improvements in the effectiveness of DOE cyber security.

- Office of Security, in conjunction with Office of CIO, has recently begun a localized desk-top computer and Local Area Network modernization effort that will serve as the pilot effort for the DOE aimed at improving speed, efficiency and protection of sensitive information management.

- DOE is working with DOD to implement classified communications with the DOD using the Secret Internet Protocol Routing Network (SIPRNet) employed at DOD to substantially enhance capabilities between the agencies to share and manipulate classified information.

- DOE has developed internal secure e-mail capability up to the Secret/Restricted Data level.

- Office of Security maintains a technology development program focusing on information security, which has been instrumental in development of Network Intrusion Detection capabilities for use in the DOE.

- The CIO has initiated a complementary technology development program initiative to augment the efforts of the Office of Security, but focused on broader information management requirements coordinated to avoid duplication.