Department of Energy
Washington, DC 20585

March 24, 2006

MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS

FROM: THOMAS N. PYKE JR.
CHIEF INFORMATION OFFICER

SUBJECT: Cyber Security Certification and Accreditation Guide

To assist in improving the Department's cyber security certification and accreditation practices, I am approving the attached Certification and Accreditation (C&A) Guide. This Guide was developed by the staff of the Office of the Chief Information Officer (OCIO) in collaboration with the Cyber Security Working Group, which includes broad representation across DOE. The Guide is consistent with government-wide C&A guidance issued by the National Institute of Standards and Technology. I request your help to ensure that the C&A processes within your organization, while continuing to be consistent with acceptable risk relative to your mission, are reviewed and adjusted to address the principles and concepts in this Guide as soon as possible.

Issuance of this Guide is part of initial implementation of the Department's new Cyber Security Program Revitalization Plan. Recent Office of the Inspector General (IG) and Office of Independent Oversight and Performance Assurance (SSA) reviews and assessments have identified C&A as a systemic weakness across the Department. While the concerted efforts of cyber security professionals across the Department have ensured that over 99% of our systems are accredited for operation through a C&A process, the maturity and completeness of our C&A processes remain inconsistent across the Department. This inconsistency has resulted in the majority of reviewed C&A packages being assessed as incomplete or not properly addressing the total risk to the associated information system.

The Guide is designed to assist in maturing your organization's C&A process and strengthening the resulting C&A packages. It establishes minimum principles and concepts for the certification and accreditation of all DOE information systems, and it updates and clarifies the guidance contained in DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*, and we plan to cancel DOE N 205.9. As part of OCIO's performance measurement and compliance monitoring, OCIO, in coordination with the IG and SSA, will begin assessing the implementation of this Guide and the strength of improved C&A processes and packages within DOE organizations by late summer of 2006.

Our office is available to provide advice and assistance to your staff on the implementation of the Guide's principles and concepts into your C&A processes and practices. Gordon Errington, Deputy CIO and Acting Associate CIO for Cyber Security, can be reached at (202) 586-0166.

Printed with soy ink on recycled paper

Thank you for your personal attention to ensuring that the content of this new Guide is integrated into your organization's cyber security program as soon as possible. As we continue to work together to improve DOE's cyber security posture, increasing the strength of C&A processes across the Department is essential to our success.

Attachment