

February 2, 2007

MEMORANDUM TO: Chairman Klein  
Commissioner McGaffigan  
Commissioner Merrifield  
Commissioner Jaczko  
Commissioner Lyons

FROM: Luis A. Reyes */RA/*  
Executive Director for Operations

SUBJECT: CHANGE IN PRIORITIES OF THE NUCLEAR REGULATORY  
COMMISSION'S CERTIFICATION AND ACCREDITATION OF  
INFORMATION TECHNOLOGY SYSTEMS

This memorandum requests Commission approval to change the priorities of the staff's efforts to certify and accredit information technology (IT) systems. This change is consistent with guidance recently received from the Office of Management and Budget (OMB) staff following their review of the NRC system descriptions and business cases (Exhibit 300s) provided with the agency FY 2008 budget request.

As background, in September 2005, the NRC's Office of the Inspector General (OIG) evaluation of NRC's implementation of the Federal Information Security Management Act (FISMA) found that the majority of the agency's IT systems were operating under an Interim Authority to Operate (IATO), which does not convey full accreditation. In response to the OIG evaluation and direction from former Chairman Diaz, the NRC's approach to the Certification and Accreditation (C&A) process was adjusted to place priority on financial systems and infrastructure systems, all of which are legacy systems.

In a December 15, 2005, memorandum, former Chairman Diaz directed the staff to "...refocus the accreditation and certification activities on the highest priority systems that are mission critical and those that potentially pose a higher security risk." The first five systems prioritized to obtain an Authority to Operate (ATO) were License Fees Reporting System (Fees), National Source Tracking System (NSTS), Human Resources Management System (HRMS), Local Area Network/Wide Area Network (LAN/WAN), and Data Center System (DCS).

CONTACT: Myron Kemerer, OIS/BPIAD  
(301) 415-8735

Staff met with OMB on December 12, 2006, to discuss NRC's OMB Exhibit 300, FY 2008 passback scores. The meeting's focus was on whether C&A had been completed and an ATO issued for all of the 25 major investments represented in Exhibit 300s. OMB staff suggested it would be more fiscally responsible to redirect our resources being expended to document legacy systems with limited existing documentation, towards accelerating planned system modernizations of legacy systems that will be designed to achieve an ATO. The information gained in applying the current approach for C&A demonstrates that it is costly and labor-intensive to re-create documentation for systems which have modernization plans. Therefore, the staff recommends that we re-focus attention to newer systems which can be certified within a shorter time frame and lower cost. The Software Engineering Institute endorses this approach.

This re-prioritization approach will result in four systems being accredited (ATO) by the end of March 2007 (Digital Data Management System, Licensing Support Network, Operations Center Information Management System, and Reactor Program System) as shown in the enclosure. For the remaining 43 systems, OIS will work with the legacy system owners to evaluate the risk of re-focusing on modernization and determine the best course forward. The plan is to accredit a total of 12 systems by the end of FY 2007 and accredit the remaining 31 systems by the end of FY 2009.

OIS and system owners for the four systems to be accredited in March 2007 have begun work on these systems and on the National Source Tracking System. The Software Engineering Institute, which is providing independent advisory assistance to the Chief Information Officer, finds no reason to disagree with this approach as it will prioritize resources and bring immediate benefits to new system developments. With Commission approval of this change in priorities approach, staff will work to fully implement this proposal.

This memorandum neither requests nor anticipates additional resources. The Office of Chief Financial Officer has reviewed this memorandum for resource implications and has no objections. The Office of the General Counsel has no legal objections to the recommendations in this memorandum.

SECY, please track.

Enclosure:  
Re-focused C&A Schedule

cc:    SECY  
       OGC  
       OCA  
       OPA  
       CFO

## Re-focused Certification and Accreditation Schedule

System	System Acronym	Step Completed	Fiscal Year Scheduled for ATO	Qtr
Digital Data Management System	DDMS	1	2007	Qtr 2
Licensing Support Network	LSN	1	2007	Qtr 2
Reactor Program System	RPS	2	2007	Qtr 2
Operations Center Information Management System	OCIMS	1	2007	Qtr 2
Secure Payment System (FMS)	SPS		2007	Qtr 4
Data Center Services	DCS	2	2007	Qtr 4
Remote Access System	RAS		2007	Qtr 4
Local Area Network/ Wide Area Network	LAN/ WAN	2	2007	Qtr 4
NRC System Information Control Database	NSICD	1	2007	Qtr 4
Cost Accounting System	CAS	2	2007	Qtr 4
Electronic Questionnaire for Investigations Processing <sup>1</sup>	EQUIP		2007	Qtr 4
Budget Formulation Application <sup>1</sup>	BFA	2	2007	Qtr 4
License Fee Reporting System <sup>2</sup>	FEES	2	2007	
Human Resources Management System <sup>2</sup>	HRMS	2	2007	
Integrated Personnel Security System	IPSS		2008	
Federal Financial System (DOI/NBC)	FFS	1	2008	
Federal Personnel & Payroll System (DOI/NBC)	FPPS	1	2008	
NIH Mainframe Host System	NIH		2008	
3-Tier Web Services	3-Tier		2008	
Email Services	Email		2008	
Intrusion Detection System and Security Devices	IDSSD		2008	
LIMIT 30 W. Gude Drive, Rockville, MD	LIMIT-Gude		2008	
Managed Public Key Infrastructure	MPKI	1	2008	
Telecommunications System	TELECOM		2008	
Web Servers	Web Servers		2008	
Windows Servers	Windows Servers		2008	
Electronic Hearing Docket	EHD		2008	
Federal Procurement Data Systems-Next Generation	FPDS-NG		2009	
General License Tracking System	GLTS		2009	
License Tracking System	LTS		2009	
National Source Tracking System (Safesource Phase 2)	NSTS	1	2009	
Center for Nuclear Waste Regulatory Analyses	CNWRA		2009	
Emergency Response Data System	ERDS	1	2009	
Idaho National Engineering and Environmental Laboratory	INEEL		2009	
S&G Electronic Safe	S&G ESafe		2009	
S&G Local Area Network	S&G LAN		2009	
OIG Management Information System	OIGMIS		2009	
Novell Servers	Novell Servers		2009	
Agencywide Document Access and Management System	ADAMS	2	2009	
Consolidated Test Facility	CTF		2009	
Databases	DB		2009	
Managed Desktops and Laptops	DESKTOPS		2009	
Electronic Information Exchange	EIE		2009	
L3-EER 1098 Taft St., Rockville, MD 20850	L3-EER		2009	
Technical Assessment Center	TAC		2009	
Unix Servers	Unix Servers		2009	
Code Development System	HPCS-CDS/CFD	1	2009	
Booz Allen Hamilton McLean Facility	BAH-McLean	6		
Grant Thornton Facility	Grant	6		

**Step 1 - SecCat; Step 2- Risk Assessment; Step 3 -System Security Plan; Step 4- ST&E;**  
**Remediation of Significant Vulnerabilities; Step 6 - ATO**

**Step 5**