ADAMS ML070180024

# U.S. Nuclear Regulatory Commission

# Privacy Impact Assessment

(*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)*

# for the

# Digital Data Management System

**Date:** January 8, 2007

## A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

The DDMS is a hearing support system that combines web-based document management with digital evidence presentation/recording to provide users with access to searchable evidentiary material, including video transcripts, and a means to present most evidentiary material electronically. Although primarily a system for litigants, the DDMS also provide the public with greater public access to ASLBP hearings by providing large-screen monitors display of evidentiary materials and internet-available web broadcasts of hearing sessions. DDMS also permits greater access for disabled persons by providing closed-captioning, assisted listening, and compatibility with computer screen-reading technology.

Because the system was developed using a standard web interface, users can access DDMS from the ASLBP Rockville, Maryland hearing room, the ASLBP Las Vegas, Nevada hearing facility, a "remote" hearing site, or wherever they are able to establish an Internet connection.

Specifically, DDMS:

A. Provides information technology (IT) and audio/visual (A/V) capabilities in the ASLBP's Rockville and Las Vegas hearing rooms and, potentially, other "remote" locations where hearings are conducted;
B. Enables the creation and use of an integrated, comprehensive digital record for agency licensing and enforcement cases;
C. Records, stores, and displays the text and image of documents presented in a hearing using pre-filed electronic documents from the Electronic Hearing Docket (EHD);

D. Permits access and retrieval of the entire record, including (1) already docketed documentary material, transcripts, and exhibits; (2) previously recorded A/V presentations or computer simulations; and (4) hearing session testimony;
E. Allows counsel for the parties to bring electronically prepared evidentiary material to the hearing and have it integrated into the record and accessible in the hearing room;
F. Provides almost continual, virtually real-time access to the hearing record by the presiding officer and parties to the litigation;
G. Supports pre-hearing, hearing, and post-hearing information management (IM) for the Licensing Board proceeding and any subsequent agency and judicial appellate processes;
H. Is consistent with the Commission's procedural rules and policies;
I. Enhances the ability of the Licensing Board and the litigants to conduct efficient and effective hearings;
J. Provides enhanced public access to information used during the hearing; and
K. Improves litigant and public perceptions of the NRC adjudicatory process.

2. What agency function does it support?

DDMS improves the ability of the NRC to conduct business electronically with external entities and employs techniques to process and make available, the entire adjudicatory record electronically, reducing paper and manual processes. It employs teleconference and videoconference technologies to make NRC staff, witness and party participation more flexible. Additionally, it provides external stakeholders the ability to access the agency's publicly available information more easily and effectively.

3. Describe any modules or subsystems, where relevant, and their functions.

**Hearing Management**
The DDMS Hearing Management subsystem administers, at a high level, the information associated with the hearing itself. This includes calendaring, scheduling, report generators, authoring tools, and other functions related to hearing management. Other functions include capturing dispositional information, along with managing and linking lists and other information about witnesses, depositions, exhibits, and issues. Finally, the hearing management software securely manages protective orders in such a way as to prevent tampering and unauthorized disclosure.

**Document/Object Management**

The DDMS Document/Object Management subsystem is implemented using the Plumtree Corporate Portal[1] product. This product, in turn, uses Microsoft SQL Server to manage the documents and objects within the DDMS. Through the DDMS portal - which provides the primary user interface - users can locate any document within the DDMS according to their access permissions. The Document/Object Management subsystem also maintains (as a series of project files) the record of each day's proceeding. This record includes the objects (exhibits) references, the official transcript, scheduled and actual witness appearances, the video file, and any other documents pertaining to the hearing.

The Web/Portal Server (running Plumtree software and supporting the Document/Object Management subsystem) hosts the interfaces between the DDMS and the rest of the NRC. These include interfaces with the EHD, which allows the DDMS to receive pre-filed materials submitted to ADAMS via the NRC's Electronic Information Exchange (EIE) server. This server also provides users an interface to external information providers defined to be only Lexis/Nexis, Westlaw, the Licensing Support Network, and the NRC official web site. Through this interface point, internal DDMS users are allowed access to these pre-defined services in a secure environment that constrains the specific sites that users can utilize through the use of IP filtering on the DDMS boarder routers. These latter functions, while characterized as Document/Object Management, also support the Hearing Management environment

**Multimedia Management**

The hearing's live video feed is routed into a video switcher. The switcher is sound activated to provide automatic camera switching to capture the current speaker. In the event that a clerk needs to manually switch camera views, an override capability is provided to allow for manual camera switching. The system is also configured such that the audio can be either automatically or manually switched with a manual override/muting capability. The switched video feed becomes the official hearing record and provides synchronization of the official hearing transcript as well as all evidence to the switched video feed.

The composite output of the switched video feed is routed to the indexing and encoding subsystem. It is then synchronized with the real-time text transcript feed from the court reporter position. Following indexing, the DDMS encoding feature converts the composite video feeds to digital video for storage in the video server and storage subsystems.

The digital video is stored in the video server and storage subsystem in Windows Media Video format. The video server and storage subsystem also contains a transcoding system and streaming media server(s) to allow for low-resolution viewing of video to authorized DDMS users accessing DDMS from the hearing room or over the internet.

---

[1] Note: The Plumtree Portal suite of products was purchased by BEA Systems, Inc. BEA renamed the Plumtree Portal suite of products to BEA AquaLogic™ User Interaction.

4. Points of Contact:

| **Project Manager** | **Office/Division/Branch** | **Telephone** |
|---|---|---|
| Andrew Welkie | ASLBP | 415-6541 |
| **Business Project Manager** | **Office/Division/Branch** | **Telephone** |
| Daniel J. Graser | ASLBP | 415-7401 |
| **Technical Project Manager** | **Office/Division/Branch** | **Telephone** |
| Andrew Welkie | ASLBP | 415-6541 |
| **Executive Sponsor** | **Office/Division/Branch** | **Telephone** |
| E. Roy Hawkens | ASLBP | 415-7550 |

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System __X__ Other (Explain)

The Digital Data Management System (DDMS) was developed for use in the HLW proceeding with the eventual intent of using it for all ASLBP proceedings. The documentation regarding the data source for DDMS, which is EHD, mixes references to HLW-EHD and EHD. OIS has merged HLW-EHD and EHD into just EHD for both general proceeding data and HLW data. In an effort to bring DDMS in line with that change as well as clarify the use of DDMS for use in both the HLW proceeding and general proceedings , we have begun revising our documentation to reflect references to EHD for the source of DDMS data. Essentially, the nature of the data that DDMS will process does not change and the data sensitivity of the DDMS data remains the same. In documentation space, we replaced all references of HLW-EHD to just EHD, since the data origination point and destination of data for the HLW proceeding and general proceedings from the DDMS perspective is the same.

b. If modifying an existing system, has a PIA been prepared before?

Yes

(1) If yes, provide the date approved and ADAMS accession number.

It was approved on November 8, 2005 and the ADAMS access number is ML052970039.

## B. INFORMATION COLLECTED AND MAINTAINED

*(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is*

*being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)*

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system collect information about individuals?

No

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

b. What information is being maintained in the system about individuals (describe in detail)?

c. Is the information being collected from the subject individuals?

(1) If yes, what information is being collected from the individuals?

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

(1) If yes, does the information collection have OMB approval?

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from internal files, databases, or systems?

(1) If yes, identify the files/databases/systems and the information being collected.

f. Is the information being collected from an external sources(s)?

(1) If yes, what is the source(s) and what type of information is being collected?

g. How will this information be verified as current, accurate, and complete?

h. How will the information be collected (e.g. form, data transfer)?

I. What legal authority authorizes the collection of this information?

j. What is the purpose for collecting this information?

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. What type of information will be maintained in this system (describe in detail)?

Based on the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-60 and as documented in the Enterprise DDMS Security Categorization Document, the DDMS process the following types of Information:

| Information Type | NIST SP 800-60 Description |
|---|---|
| Knowledge Dissemination Information Type | Knowledge Dissemination addresses those instances where the primary method used in delivering a service is through the publishing or broadcasting of information, such as the Voice of America or web-based museums maintained by the Smithsonian. Knowledge Dissemination is not intended to address circumstances where the publication of information is a by-product of a mission rather than the mission itself. |
| Legal Prosecution/Litigation Information Type | Legal prosecution/litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility. |
| Permits and Licensing Information Type | Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function. |
| Legal Investigation Information Type | Legal investigation supports activities associated with gathering information about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence. |
| Judicial Hearing Information Type | Judicial hearings include activities associated with conducting a hearing in a court of law to settle a dispute. |

| | |
|---|---|
| Rule Publication Information Type | Rule Publication includes all activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations. |

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

**Transfer Process - Documents from EHD**
The EHD extraction program will be executed daily at pre-defined intervals. During execution, all documents newly present since the last execution will be identified using the unique EHD ADAMS_Accession_Number field. The program will then extract or export each of these identified files, along with their respective metadata, from their respective folders within FileNet's Panagon system, and place them into the comparably named file folders in the HLW_EHD_New_Content file share, creating new folders for new boards as necessary. The HLW_EHD_New_Content exists on DDMS-SRV4 server. DDMS will provide a DDMS user account named ehdpub and this user account will be granted access to the \\ DDMS-SRV4\ HLW_EHD_New_Content file share.

DDMS will crawl the folder structure in the HLW_EHD_New_Content file share and index all new documents and apply any new metadata or metadata changed as presented in the XML files.

*(Above references to HLW are part of a folder path and can not be changed.)*

**Ad Hoc Documents**
The Clerk has the ability to create a document during the hearing. These exhibits are called Ad-Hoc Documents. When the Clerk selects "Create New Document" from the Common Tasks portlet, a Create Document window displays, allowing the Clerk to select the appropriate document from the Ad-Hoc document folder mapped to the "O:" drive. Once the document is found, the Clerk selects "Next" and additional document metadata can be entered.

**Document Properties**
The Clerk also has the ability to set document metadata when creating the document. The Clerk will enter as much data as is known at the time of document creation. The Party Exhibit # data entry field includes a drop-down list restricting data entry to a known party identifier. Once the document is created, the metadata cannot be edited within DDMS.

**Video Signal Flow and Capture**
The following figure depicts the flow of the video thru the DDMS. This approach provides for the digital encoding and indexing of incoming video, stripping out the Line 21 text provided by the Court Reporter, and

synchronization of the text with the encoded video. The design also provides for a live feed with real-time playback capabilities.

c. What is the purpose for collecting this information?

The purpose of using the information processed by the Enterprise DDMS is to enable the creation and use of an integrated, comprehensive digital record for ASLBP proceedings; record, store, and display the text and image of documents presented in the hearing; permit access and retrieval of the entire record, including transcripts, exhibits, presented evidence captured through digital recording, and searchable video recording; allow counsel to present evidence electronically during the hearing; and provide continual real-time access to the hearing record.

## C. USES OF SYSTEM AND INFORMATION

*(These questions will identify the use of the information and the accuracy of the data being used.)*

1. Describe all uses made of the information.

The purpose of using the information processed by the Enterprise DDMS is to enable the creation and use of an integrated, comprehensive digital record for ASLBP proceedings; record, store, and display the text and image of documents presented in the hearing; permit access and retrieval of the entire record, including transcripts, exhibits, presented evidence captured through digital recording, and searchable video recording; allow counsel to present evidence electronically during the hearing; and provide continual real-time access to the hearing record.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

Yes

3. Who will ensure the proper use of the information?

DDMS is a hearing management tool and access is restricted only to individuals who meet, at a minimum, all of the following criteria:

1. Users must have a current EIE-issued Verisign Certificate;
2. Users must have filed a notice of appearance (see 10 C.F.R. § 2.314(b));
3. Users must attend an ASLBP-sponsored DDMS Training Session;
4. Users must be approved by the Chief Administrative Judge.

Additionally users who have access to sensitive unclassified non-safeguards information are subject to a protective order issued by the hearing board and are required to sign a confidentiality and non-disclosure agreement.

4. Are the data elements described in detail and documented?

   Yes

   a. If yes, what is the name of the document that contains this information and where is it located?

      The Enterprise DDMS Data Definition document which is located in ADAMS. ADAMS Accession Number: ML070080488 (limited access).

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

   No

   a. If yes, how will aggregated data be maintained, filed, and utilized?

   b. How will aggregated data be validated for relevance and accuracy?

   c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will the information be *retrieved* from the system (be specific)?

   DDMS is a web-based portal system providing user access through a standard web interface over a Secure Socket Layer (SSL) connection. Whether accessed from the hearing room or remotely from a user's office, DDMS is accessed with a standard desktop browser, such as Internet Explorer.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

   No

   a. If yes, explain.

      (1) What controls will be used to prevent unauthorized monitoring?

8. Describe the report(s) that will be produced from this system.

The Enterprise DDMS utilizes Crystal Reports for creating reports. There are pre-formatted available and ad-hoc reports can be created as needed. The following reports are currently available in DDMS: Daily Exhibit Report; Daily Witness Appearances Report; Scheduled; Document Appearances Report; Party Report; Proceeding Report; Official Exhibit Number Report; Witness Report; Contention Report; Scheduled Exhibits Report; Exhibit Status Report; Compound Documents Report; Hearings by Location; Hearings by Board; and Hearings by Issue.

a. What are the reports used for?

Calendar based reports are built around the calendar functions of Enterprise DDMS and provide a daily, weekly, monthly, quarterly, or yearly view of time or date-based information. Each report shows the selected information in the specified date format. Time and date-based information within Enterprise DDMS includes: boards, contentions, judges, documents, witnesses, locations, and some selected metadata information.

Summary type reports summarize information at any hierarchical level selected by the user. Organizational levels are used to categorize the information within Enterprise DDMS into manageable and related blocks of information. Organizational categories include: Proceedings selection, boards, contentions, judges, witness appearances, document-types, and locations. Information can be retrieved and grouped at any or multiple levels. Most of these reports offer parameter selection when chosen.

Performance/System Reports are used to address miscellaneous performance and system-related activities. These include error reports displaying status and any errors generated during the running of any routine DDMS jobs or crawlers. Other reports in this category could include traffic and performance statistics, auditing and security reports, and user group and community listings.

b. Who has access to these reports?

Access to reports is restricted based upon user and group roles.

## D. RECORDS RETENTION AND DISPOSAL

*(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "*NRC Comprehensive Records Disposition Schedule*.")*

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

No

a. If yes, list the disposition schedule.

2. Is there a General Records Schedule (GRS) that applies to information in this system?

No

a. If yes, list the disposition schedule.

3. If you answered no to questions 1 and 2, complete NRC Form 637, NRC Electronic Information System Records Scheduling Survey, and submit it with this PIA.

## E. ACCESS TO DATA

### 1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

The Office of General Counsel, ASLBP, and OIS

(1) For what purpose?

Conducting and participating in ASLBP proceedings.

(2) Will access be limited?

Yes. See response to C.3.

b. Will other systems share or have access to information in the system?

The DDMS will receive its data from the EHD. Documents processed during the hearing will be exported and processed into ADAMS. This transfer, whether pushed or pulled, is initiated by a process running on a system on the NRC's LAN/WAN.

c. How will information be transmitted or disclosed?

Information is transferred using a Federal Information Processing Standard (FIPS) 140-2 compliant transfer protocol.

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

The Enterprise DDMS has an Interface Control Document that governs system inter-connectivity. Users who access the information using a standard web browser must meet the criteria described in the response to C.3. Additionally, hearing participants are subject to orders issued by the Board on how DDMS is used for ASLBP hearings.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes

(1) If yes, where?

All documents are in ADAMS with limited access (with the exception of one which is still in draft) and the specific documents are:

| Document | ADAMS Accession Number |
|---|---|
| Enterprise DDMS Design Document | ML053470136 |
| Enterprise DDMS Operational Support Guide | ML053470138 |
| Enterprise DDMS Users Guide | ML053470150 |
| Enterprise DDMS Interface Control Document | ML053470129 |
| ASLBP DDMS Policies and Procedures | Draft |

2. **EXTERNAL ACCESS**

a. Will external agencies/organizations/public share or have access to the information in this system?

Yes

(1) If yes, who.

Participants in ASLBP proceedings.

b. What information will be shared/disclosed and for what purpose?

Participants in ASLBP proceedings, who are authorized DDMS users will have access information needed to conduct and participate in ASLBP proceedings.

c. How will this information be transmitted/disclosed?

DDMS is a web-based portal system providing user access through a standard web interface over a Secure Socket Layer (SSL) connection. Whether accessed from the hearing room or remotely from a user's office, DDMS is accessed with a standard desktop browser, such as Internet Explorer.

## F. TECHNICAL ACCESS AND SECURITY

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

Users authenticate using a two-factor authentication mechanism. This mechanism incorporates the use of EIE assigned client digital certificates in combination with DDMS assigned username and strong passwords. Users located within the ASLBP Hearing Rooms will not be required to present their digital certificate due to the physical security that will exist at each site.

User accounts will be created within Active Directory where password complexity and expiration policies are enforced.

A user session connecting to DDMS through the DMZ will be prompted to present their client certificate for authentication. Upon acceptance of the client certificate by the web server the user session will then be presented with the Portal login screen requiring a valid user name and strong password to gain access to the DDMS.

2. Will the system be accessed or operated at more than one location (site)?

Yes

a. If yes, how will consistent use be maintained at all sites?

Two DDMS sites, Rockville and Las Vegas, will be interconnected initially by means of a T1 connection operating at 1.544 Mbps and will potentially scale to a T3 connection operating at 45 Mbps during the HLW hearings. The link between the two sites will carry replicated data including Active Directory, database, video files, and XML files using a combination of Microsoft File Replication Services, Active Directory Replication, and SQL Server Database Replication. In addition a live video feed will be made available for both sites across the inter-site connection.

3. Which user group(s) (e.g., system administrators, project manager, etc.) have access to the system?

   The Enterprise DDMS project team has access to DDMS as well as the ASLBP staff members designated as Clerks of Court. Access to processes in the system are defined by the role a particular group has in the operation of DDMS.

4. Will a record of their access to the system be captured?

   Yes

   a. If yes, what will be collected?

   The Enterprise DDMS system logs capture a wide variety of audit information including but not limited to login/logout activity; service stop/start activity; file access etc.

   Within the DDMS application, user account information is collected when documents are processed.

5. Will contractors have access to the system?

   Yes

   a. If yes, for what purpose?

      Per the Enterprise DDMS Operations and Maintenance contract, the contractor, Nortel Government Solutions, is responsible for all aspects of the Enterprise DDMS operation.

      - Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

        - 52.224-1 Privacy Act Notification.

        - 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

   The Enterprise DDMS follows Management Directive 12.5 and all applicable Federal Guidelines for securing an information system that has been categorized as a moderate system. Complete details regarding the Enterprise DDMS

Security controls con be found in the Enterprise DDMS System Security Plan, ADAMS Accession Number ML053470143 (limited access).

7. Are the data secured in accordance with FISMA requirements?

Yes

a. If yes, when was Certification and Accreditation last completed?

Scheduled to be complete by May 2007.

**PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL**
*(For Use by OIS/IRSD/RFPSB Staff)*

**System Name:** Digital Data Management System (DDMS)

**Submitting Office:** Atomic Safety and Licensing Board Panel (ASLBP)

## A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable.

____ Privacy Act is applicable. Currently covered under System of Records, NRC- . No modification to the system notice is required.

____ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

____ Privacy Act is applicable. Currently covered under System of Records, NRC- . Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

**Comments:**

The DDMS is a hearing management tool providing access to hearing related documents through the Electronic Hearing Docket, IT and audio/visual capabilities at hearing locations, scheduling, etc. Videos of hearings are maintained in the DDMS, however the transcripts are processed into ADAMS as official agency records. The DDMS maintains information about documents (metadata).

| Reviewer's Name | Title | Date |
|---|---|---|
| Sandra S. Northern | Privacy Program Officer | January 23, 2007 |

## B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No. _____

**Comments:**

The Digital Data Management System is an NRC hearing support system that captures information relating to NRC litigation and hearings. No OMB clearance is required for this system.

| Reviewer's Name | Title | Date |
|---|---|---|
| Christopher J. Colburn | Team Leader, ICT | January 31, 2007 |

## C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

____ Existing records retention and disposition schedule covers the system - no modifications needed.

____ Records retention and disposition schedule must be modified to reflect the following:

**Comments:**

This is a significant system with numerous types of records that must be scheduled. Further review and discussion will be required to establish proposed records disposition schedules. However, this further review does not preclude moving forward with certification of the DDMS system.

| Reviewer's Name | Title | Date |
|---|---|---|
| Jeffrey L. Bartlett | Senior Records Analyst | 1/31/07 |

**D. BRANCH CHIEF REVIEW AND CONCURRENCE**

__X__ Does not constitute a Privacy Impact Assessment required by the E-Government Act of 2002

____ Does constitute a Privacy Impact Assessment required by the E-Government Act of 2002 and requires approval of the Director, IRSD.

**CONCUR IN REVIEW:** ***/RA/*** Date 1/31/2007
Margaret A. Janney, Chief
Records and FOIA/Privacy Services Branch

**E. DIVISION DIRECTOR APPROVAL OF PRIVACY IMPACT ASSESSMENT** (*If required, refer to D. above.)*

_____ Date _____
John J. Linehan, Director, Information and Records Services Division

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/**
**PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

<table>
<tr><td>TO: (Sponsoring Office)<br>Atomic Safety and Licensing Board Panel (ASLBP)</td><td colspan="2">Office Sponsor:<br>E. Roy Hawkens, Chief Administrative Judge, ASLBP</td></tr>
<tr><td>James C. Corbett, Director<br>Business Process Improvement and Applications Division, OIS</td><td colspan="2">Name of System:<br>Digital Data Management System (DDMS)</td></tr>
<tr><td>Kathy L. Lyons-Burke, CISSP<br>Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO)<br>Office of Information Services</td><td>Date RFPSB Received:<br><br>January 10, 2007</td><td>Date RFPSB Completed Review:<br><br>January 31, 2007</td></tr>
<tr><td colspan="3">Noted Application Development and System Security Issues:<br><br>No Privacy Act issues.<br><br>No information collection issues.<br><br>Further review and discussion will be required to establish proposed records disposition schedules. However, this further review does not preclude moving forward with certification of the DDMS system.</td></tr>
<tr><td>Margaret A. Janney, Chief<br>Records and FOIA/Privacy Services Branch<br>Office of Information Services</td><td>Signature: /RA/</td><td>Date: 01/31/2007</td></tr>
</table>