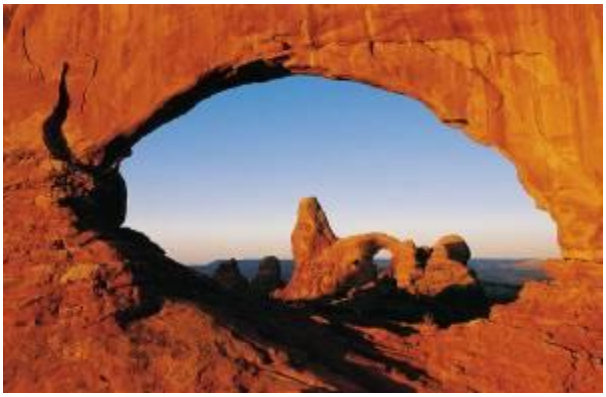
Department of the Interior
Bureau of Land Management

Information System Decommissioning Guide

Version Control Log

Date	Version #	Author	Description
January 11, 2011	0.1	WO-550	Original version
April 28, 2011	0.2	WO-550	Incorporated comments from WO-550 Division Chief
May 18, 2011	0.3	WO-550	Incorporated comments from WO-550 Division Chief
July 12, 2011	0.4	WO-550	Incorporated comments from WO-550 Division Chief
August 12, 2011	1.0	WO-550	Released

Updates to this document: The Bureau of Land Management (BLM) recognizes that the Information System Decommissioning Guide will be continually updated to improve integration with other processes (e.g., configuration and change control processes). As guidance for these and other processes are promulgated/updated, the Information System Decommissioning Guide will be reviewed for possible impacts and recommended changes.

To make suggestions for enhancement, please contact the BLM Office of the Assistant Director Information Resources Management, Division of Investment Management (WO-550).

Table of Contents

Executive Summary

The Bureau of Land Management (BLM) provides essential services to citizens and has established highly effective support systems that enable delivery of these services. As business needs and technology continue to evolve, these support systems must also evolve in tandem with the business and as a result obsolete and inadequate systems are retired and decommissioned.

The Information Systems Decommissioning Guide has been established to minimize risks and negative impacts associated with decommissioning information systems. Information in this Guide and accompanying directive are provided to:

- Minimize risks to the Bureau and Offices;
- Ensure that decommissioning activities are consistent across the BLM; and,
- Comply with applicable federal regulations and BLM policies.

System decommissioning is the termination of a system's operations. The structured procedures contained in this guide provide a step-by-step approach for ending information system operations in a planned and orderly manner. These procedures ensure that:

- Associated Information Technology (IT) hardware is properly assessed for possible re-use or disposal;
- Adequate system documentation is archived;
- Software, system logic, and data are properly archived or incorporated into receiving system(s); and,
- The approach for performing these activities is consistent and coordinated with the appropriate representatives/offices within the BLM.

Particular emphasis is given to proper data migration and preservation and to facilitating subsequent use of data by receiving/target systems. The steps taken to archive and store data are in accordance with BLM records management policies as well as National Archives and Records Administration (NARA) policies and requirements for data retention.

Decommissioning activities contained in this methodology consist of:

- Establishing a migration plan;
- Performing migration activities;
- Establishing a decommission plan;
- Performing the decommission; and,
- Performing a post-decommission review.

Preface

Purpose
This Information System Decommissioning Guide was created by the BLM to establish a standardized, systematic approach for retiring information systems.

Scope
This guide applies to all BLM-owned or BLM-funded information systems, and any supporting information technology, undergoing decommissioning (planned, or in progress) must follow the process outlined in the Information System Decommissioning Guide. This IM also impacts other systems affected by the decommissioning of a particular system (e.g., receiving/target systems that support the business functions of, or maintain data transitioning from a decommissioned system).

Information System Decommissioning Process

This document describes specific system decommissioning activities, identifies who should be involved at each step, and provides guidelines and templates for documents to be created during each activity.

The high-level process for system decommissioning may require migrating to a receiving/target system data or business functions that have been supported by a legacy system that is to be decommissioned. In this case, the transition requires that a migration plan be established and those migration tasks be completed before the legacy system is decommissioned. At the end of the migration process, designated BLM representatives/Offices sign a certificate of migration acknowledging that all migration activities have been successfully performed.

Once the certificate of migration has been signed, decommissioning plan development and subsequent decommissioning activities can be performed to terminate operations of the legacy system. At the end of the decommissioning process, those same designated BLM representatives/Offices sign an additional certificate of decommissioning acknowledging that all decommissioning activities have been successfully performed. The final step in the decommissioning process is to perform a review to ensure that all necessary requirements for decommissioning the system have been successfully accomplished.

When it is not necessary to transition legacy system data or functions to a receiving/target system, the legacy system may be decommissioned without completing migration activities. In this case, there are three basic steps:

- Develop a decommission plan,
- Perform the decommissioning activities, and
- Complete a final post-decommission review.

Figure 1 (on the following page) depicts the high-level process flow for both decommissioning scenarios. More detailed descriptions of individual steps are provided in the subsequent sections of this document.

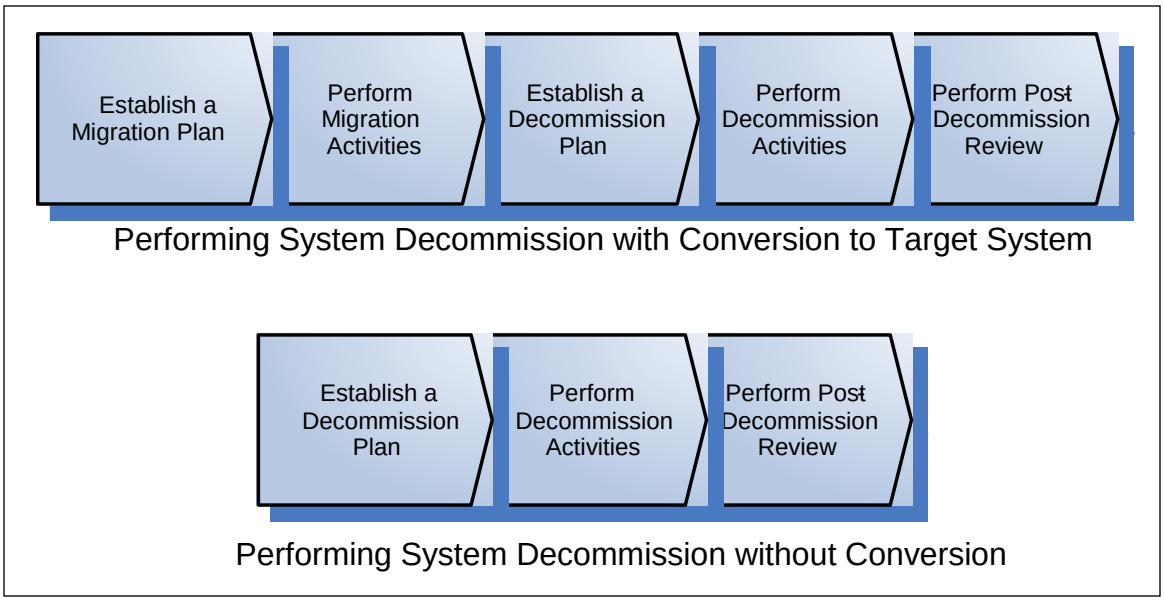


Figure 1: Decommissioning Process Overview

Establish a Migration Plan

In many cases, a system that is being decommissioned encompasses processes, workflows, logic, or data that must be migrated to a receiving/target system. For this reason, it is important that the system that will be decommissioned is first adequately migrated in terms of its functionality and data. Where a migration to a receiving/target system is scheduled, each system should have a migration plan that is developed and signed off by the project manager responsible for the decommissioning, the system owner for the legacy system, the BLM Assistant Director, Information Resources Management (ADIRM), for both the decommissioning system and/or target/receiving system, the BLM Chief Information Security Officer, the BLM Chief Architect, and the system owner for the receiving/target system. The migration plan should be established and signed off prior to conducting migration activities.

The document to be created during this activity is the Migration Plan. This document, along with the Migration Certificate and other project artifacts (e.g., project schedule, communications plan), should be maintained as part of the project file by the project manager of the legacy system that is to be decommissioned.

A template for the Migration Plan is provided in Appendix A. The plan also should include the elements shown on the next three pages in Table 1.

Table 1: Migration Plan Elements

Elements of a Migration Plan	Description
Date	Document the date that the migration plan form was developed.
Project Manager Information	Identify the project manager responsible for performing the migration activities, including name, office, email address, and telephone.
Legacy System Information	Identify the legacy system name and DEAR/CSAM ID.
Legacy System Overview	Provide an overview of the system undergoing migration. Describe the general nature or type of system, including a brief overview of the business functions the system currently supports (mappings to the business reference model (BRM)), processes, and high-level workflow. Discuss the type of data (e.g., information classes/data subject areas) maintained in the legacy system (mappings to the data reference model (DRM)).
Receiving/Target System Information	Identify the receiving system name and DEAR/CSAM ID.
Receiving/Target System Overview	Provide an overview of the receiving/target system. Describe the general nature or type of system, including a brief overview of the business functions from the legacy system that will be supported by the target system (mappings to the BRM). Discuss the type of data (e.g., information classes/data subject areas) maintained in the legacy system that will be migrated to be included in the target system (mappings to the DRM).
Migration Overview	Describe the legacy system structure and major components and designates which system components will and will not be migrated. If the migration process will be organized into discrete phases, identify which system components will undergo migration in each phase. Address in explicit subsections the migration overview associated with hardware, software, and data, as appropriate. Specifically, list each of the BRM, service reference model (SRM), DRM, and technical reference model (TRM) mappings with details as to where and when they will be migrated to the receiving/target system. Include a milestone chart for the migration process.
Migration Requirements	List any special requirements for the migration and detail what is required to be migrated, who is responsible for setting each requirement, and whether any of the requirements will be delayed beyond the original migration schedule.
Hardware Migration Overview	Provide a detailed description of the migration from legacy system hardware and describe the legacy hardware that will no longer be used and the receiving/target hardware to which the system is being migrated. Map the legacy hardware to the receiving/target hardware. Also, be sure to describe any specific requirements for media sanitization, as required by NIST SP 800-88, Guidelines for Media Sanitization.
Software Migration Overview	Describe the migration from the legacy system software, the legacy software that will no longer be used and the receiving/target software to which the system is being migrated. Map the legacy software to the receiving/target software.

Elements of a Migration Plan	Description
Data Migration Overview	Describe the data migration strategy, data quality assurance, and data migration controls. Also, be sure to describe how data will be migrated, measured, and ensured; the controls that will be in place to ensure that data migration has been successful; and, any requirements associated with maintaining/transferring authoritative data source (ADS) designations or related service-level agreements (SLA). Also, describe the specific data preparation requirements and the data that must be available for the system migration. If data will be transported from the original system, provide a detailed description of the data handling, migration, and loading procedures. If the data will be transported using machine-readable media, describe the characteristics of each media component. List and account for all data mapped to the legacy system in terms of where and when it will be migrated. The target system should have the data mappings from the DRM populated. All electronic records should be managed following the National Archives regulations, NARA Records Management Guidance and Regulations, subchapter B, Record Management, Part 1234 at: http://www.archives.gov/about/regulations/part-1234.html. All records should be managed following BLM policies on records management. BLM policies can be found at: http://web.blm.gov/internal/wo-500/records/records.html. It may also be necessary to address any existing Bureau/Office-specific requirements for data retention in this section of the decommissioning plan. Consult the designated Bureau/Office Records Manager. Contact information is available at: http://web.blm.gov/internal/wo-500/records/records.html. Where applicable, this section also addresses any special requirements for publishing a notice in the Federal Register associated with the system migration, such as the requirements for NARA review of records disposition requests from federal agencies. See: http://www.archives.gov/records-mgmt/policy/records-schedule-review-process.html.
Security Overview	Describe the system security and access rights associated with the legacy system: any security features associated with the system, its network configuration, its user authorization capabilities, data-level security considerations, and any other security features, as well as how those security features will be accommodated or modified by the receiving/target system. For additional information regarding BLM Information Technology (IT) security policies, please refer to the BLM IT Security Policy at: http://web.blm.gov/internal/wo-500/security/Security.html. Emphasize and outline data security and associated risk mitigation strategies. Identify the impact-to-enterprise risk and develop a strategy for mitigating the risk. Identify the impacts to the enterprise security posture caused by the decommissioning of the system and the rationale for changes to the certification and accreditation (C&A) boundaries that are impacted by decommissioning the system. Also, identify and address impacts to common controls provided by the legacy system and the systems that rely upon those common controls. This section also includes requirements for specifying an accreditation bridge plan, if necessary, and any additional security-related requirements associated with concurrently maintaining both the legacy system and receiving/target system during the transition process.

Elements of a Migration Plan	Description
Impact to Interfaces	Describe the legacy system's interfaces to other systems that will be affected by the migration. Detail the legacy-system-to-feeder-system interfaces and the receiving/target-system-to-feeder-system interfaces. List each affected interface and the changes that will be needed in order to support or eliminate the interface upon migration.
Test Plan	Describe the testing that will be conducted to ensure that all migration activities are successful. At a minimum, include who will perform the testing, the test cases that will be performed, and how the results of the testing will be tracked and reported.
Migration Risks	Describe the major risk factors in the migration effort and strategies for their control or reduction. Describe the risk factors that could affect the migration feasibility, the technical performance of the migrated system, the migration schedule, or costs. In addition, review the current backup and recovery procedures to ensure they are adequate and operational. The project manager for the migration is responsible for mitigating identified risks.
Migration Schedule	This section contains a work breakdown schedule (WBS) consisting of activities, tasks, milestones, and a fully developed test plan. Identify critical design reviews, indicating progress of the migration itself. The WBS should be developed using project management software, such as Microsoft (MS) Project.
Migration Resources	This section describes the resources necessary to perform the migration. Highlight required hardware, software, people, and facility resources not currently available and detail an approach for obtaining all currently unavailable resources.

At the end of system migration planning, the project manager for the migration will coordinate management approvals formally documented in a migration plan approval memorandum (memo). Developed by the project manager, the migration plan approval memo is a statement that declares that the plan has been reviewed and approved. The approval memo is signed by the project manager, the legacy system owner for the legacy system, the BLM Chief Information Officer, the BLM Chief Information Security Officer, the BLM Privacy Officer, the BLM Records Officer, the BLM Chief Architect, and the system owner for the receiving/target system. The migration plan and the signed migration plan approval memo are retained by the project manager as part of the project record for the project that included within its scope the termination of the legacy system operations.

> *Note: When the legacy and receiving/target systems are owned by different Bureaus and/or Offices, signatures from both the legacy and receiving/target systems' Bureau/Office officials must be obtained.*

A template for the Migration Plan Approval Memo is provided in Appendix A.

Perform Migration Activities

This step involves the actual performance of migration activities in cases where functionality/data of the legacy system will be migrated to a receiving/target system. In such cases, the migration should be performed based on the approved migration plan. This step should not be initiated until the necessary migration resources outlined in the plan are available and risks have been accepted or mitigated.

Each migration project will be unique. Developing a migration plan and obtaining approval for the plan adds structure and quality assurance. Executing migration activities according to the plan provides accountability and traceability to ensure success. At the end of the migration, the project manager coordinates management approvals of documentation created during the activity. Management approval and acknowledgement is formally documented in the Certificate of Migration.

The Certificate of Migration, a statement declaring the success of the migration and the successful accomplishment of the activities, is developed by the project manager for the migration. This document includes signatures of the legacy system owner, the BLM Chief Information Officer, the BLM Chief Information Security Officer, the BLM Privacy Officer, the BLM Records Officer, the BLM Chief Architect, and the system owner for the target system. The intent of the Certificate of Migration is to provide assurance and justification for beginning decommissioning activities.

> *Note: When the legacy and receiving/target systems are owned by different Bureaus and/or Offices, signatures from both the legacy and receiving/target systems' Bureau/Office officials must be obtained.*

A template for the Certificate of Migration is provided in Appendix A.

Establish a Decommission Plan

The first decommissioning activity is the development of a Decommission Plan for the legacy system. The Decommission Plan ensures that the decommissioning of the legacy system is planned and executed in a way that data and application logic are preserved, affected parties are appropriately notified, and disposition of hardware and software is conducted in compliance with established federal guidelines.

Each system that is moved into a non-production state should have a Decommission Plan developed by the project manager for the decommissioning. Approval for the Decommission Plan includes: the system owner for the legacy system, the BLM ADIRM, the BLM Chief Information Security Officer, the BLM Privacy Officer, the BLM Records Officer, and the BLM Chief Architect. An approved Decommission Plan should be established prior to conducting decommission activities.

The Decommission Plan, along with the certificate of decommissioning and other project artifacts (e.g., project schedule, communications plan), should be maintained as part of the project file by the project manager of the legacy system to be decommissioned. A template for the Decommission Plan is provided in Appendix A. The plan should include the elements outlined on the next page in Table 2.

Table 2: Decommission Plan Elements

Elements of a Decommission Plan	Description
Date	Enter the date that the decommission plan form was developed.
Project Manager Information	Provide information to the project manager responsible for performing the decommissioning activities, including: name, agency (or bureau), email address, and telephone number.
Legacy System Information	Provide information for the legacy system that was decommissioned.
Legacy System Decommission Date	List the expected decommission date for the legacy system.
Date of Migration Certification	List the date that the final signature was obtained for the certificate of migration.
Software Archive Overview	Describe the plan for archiving the software library files and related documentation in the system being decommissioned, including which software will be archived, and in which format. The intent of the software archive is to provide sufficient stored software so that the system could be re-initiated if necessary. Software associated with decommissioned systems should be archived based on the records disposition schedules. More information about the BLM's records, policies, and disposition schedules is published at: http://web.blm.gov/internal/wo-500/records/records.html.
Documentation Archive Overview	Describe the plan for archiving the hard copy and soft copy user documentation for the systems being decommissioned, including which documentation will be archived and in which format. The intent of the documentation storage is to provide sufficient archived documentation so that the system could be re-initiated and used if necessary. Documentation associated with decommissioned systems should be archived based on the records disposition schedules. More information about the BLM's records, policies, and disposition schedules is published at: http://web.blm.gov/internal/wo-500/records/records.html.
Hardware Disposition Overview	This section describes the plan for disposing of hardware that was used exclusively by the decommissioned system. One source of information for hardware disposition is the Environmental Protection Agency's (EPA's) *Ecycling* program. The EPA offers Ecycling as a service to federal agencies for recycling electronics and assets. The goal of the EPA program is to help agencies recycle or properly dispose of computers and other electronic equipment in order to prevent hazardous substances inside these items from entering landfills. More information can be found at: http://www.epa.gov/epaoswer/osw/conserve/plugin/index.htm. This section also specifies any specific steps to be performed for media sanitization, as required by NIST SP 800-88, Guidelines for Media Sanitization.

Elements of a Decommission Plan	Description
Data Archive Overview	Describe the plan for archiving data files and related documentation of the system being decommissioned. The BLM has an official policy on records retention, which is in alignment with records guidance published by NARA. Any data that has not been migrated to the receiving/target system should be archived based on the BLM policy for records retention. Data archival processes also consider any requirements associated with any maintaining/transferring ADS designation or related SLA. Outline which data have been migrated, which data will be archived, and in which format. More information on the BLM records retention policy can be found at: http://web.blm.gov/internal/wo-500/records/records.html. All electronic records should be managed following the National Archives regulations, NARA Records Management Guidance and Regulations, subchapter B, Record Management, Part 1234, found at: http://www.archives.gov/about/regulations/part-1234.html. Where applicable, this section also addresses any special requirements for publishing a notice in the Federal Register associated with the system migration, such as the requirements for NARA review of records disposition requests from federal agencies at: http://www.archives.gov/records-mgmt/policy/records-schedule-review-process.html.
Security Overview	Describe the system security and access rights associated with the legacy system in order to provide the necessary security information in the decommission plan so that the system could be reconstituted with the same security considerations, if necessary. The inclusion of the legacy system's security overview ensures that the applicable security considerations become part of the archive. For additional information regarding BLM IT security policies, please refer to the BLM IT Security Policy at: http://web.blm.gov/internal/wo-500/security/Security.html. After the decision has been made to retire the system, the final system baseline is frozen and all configuration management documents are included in the information preservation process. This section also identifies the impacts to the enterprise security posture caused by the decommissioning of the system and the rationale for changes to the C&A boundaries that are impacted by the decommissioning of the system. Identify and address impacts to common controls provided by the legacy system and the systems that rely upon those common controls.
Decommission Risks	Describe the major risk factors in the decommission effort and strategies for their control or reduction. Include descriptions of risk factors that could affect the decommission feasibility, the decommission schedule, or costs. The project manager for the decommissioning is responsible for mitigating identified risks.
Decommission Schedule	Provide a WBS that consists of the activities, tasks, milestones, and review points for the decommission itself. The WBS is developed using project management software, such as MS Project.

Elements of a Decommission Plan	Description
Decommission Resources	Describe the resources necessary to perform the decommission activities, including identification of required hardware, software, people, and facility resources and a detailed approach for obtaining all currently unavailable resources. Total Cost of Ownership (TCO) and Decommissioning Cost Template must also be completed and retained as part of the project record for the decommissioning of all major systems and all systems associated with architected segments. A template is provided in Appendix A.

At the end of system decommission planning, the project manager for the decommissioning will develop and coordinate management approvals for a decommission plan approval memo, a statement that declares that the plan has been reviewed and approved. The approval memo includes the signatures of the project manager, the legacy system owner for the legacy system, the BLM Chief Information Officer, the BLM Chief Information Security Officer, the BLM Privacy Officer, the BLM Records Officer, and the BLM Chief Architect. The certificate of decommissioning is also signed by the Authorizing Official (AO), who is the official with authority to assume formal responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, as defined in NIST SP 800-53 Rev.2, Guide for Assessing the Security Controls in Federal Information Systems. The signed decommission plan approval memo, along with the decommissioning plan, is retained by the project manager as part of the project file.

A template for the Decommission Plan Approval memo is provided in Appendix A.

Perform Decommission Activities

This step is the actual performance of decommissioning activities, which should be performed according to the approved Decommission Plan. This step should not begin until necessary resources outlined in the Decommission Plan have been made available and risks have been accepted, eliminated, or mitigated. Although each decommission project will be unique, developing a Decommission Plan, obtaining approvals, and performing those activities according to plan will provide structure and accountability for the process. At the end of the decommissioning activities, the project manager for the decommissioning will coordinate management approvals that will be formally documented in the Certificate of Decommissioning.

The Certificate of Decommissioning, a statement that declares successful completion of decommissioning activities for the legacy system, is developed by the project manager for the decommissioning and includes the signatures of the project manager, the legacy system owner, the BLM ADIRM, the BLM Chief Information Security Officer, the BLM Privacy Officer, the BLM Records Officer, and the BLM Chief Architect. The Certificate of Decommissioning is also signed by the Authorizing Officer, who has the authority to assume formal responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, as defined in NIST SP

800-53 Rev.2. The intent of the Certificate of Decommissioning is to have all parties declare the success of decommission activities and to certify that the system is no longer in production.

A template for the Certificate of Decommissioning is provided in Appendix A.

Perform Post-Decommission Review

At the end of the decommissioning activities, it is important to gather lessons learned from participants and leadership in order to determine how future decommissions can be more efficient and effective. In addition to capturing lessons learned, the post-decommission review is meant to document the location of all products and documentation that have been archived.

Each system that has been decommissioned should have a post-decommission review report prepared by the project manager for the decommissioning and reviewed by the legacy system owner, the BLM ADIRM, the BLM Chief Information Security Officer, and the BLM Chief Architect. This document should be maintained by the project manager as part of official project records. A template for post-decommission review report is provided in Appendix A. The post-decommission review report should include the elements described on the page in Table 3.

Table 3: Post-Decommission Review Report

Elements of the Post-Decommission Review Report	Description
Date	Enter the date that the decommission review was completed.
Project Manager Information	Provide information to the project manager responsible for performing the decommissioning activities, including name, agency (or bureau), email address, and telephone
Legacy System Information	Provide information for legacy system that was decommissioned.
Legacy System Decommission Date	Provide the date on which the decommission activities were completed.
Date of Decommission Certification	Provide the date that the final signature was obtained for the certificate of decommissioning.
Lesson Learned: Data	Describe the migration/migration/archival of specific data/records from the legacy system that was decommissioned. If data/records from the legacy system have been archived, state the medium, format, location, and how to access the archived information. Explain any problems or mishaps that may have occurred during decommissioning of the data/records and possible preventative measures that others should consider in future decommission efforts.
Lessons Learned: Software	Describe the migration/archival/replacement/disposal of the software from the legacy system that was decommissioned. If software from the legacy system has been archived, state the medium, format, location, and how to access the archived software. Explain any problems or mishaps that may have occurred during the decommissioning of the software and preventative measures that others should consider in future decommission efforts.
Lessons Learned: Hardware	Describe the migration/disposal/re-use of the hardware from the legacy system that was decommissioned. Explain any problems or mishaps that may have occurred during decommissioning of the hardware and preventative measures that others should consider in future decommission efforts.
Archive Data	Explain where the old data is stored. If the old data was incorporated into a new system, it should be stated here. If some of the old data has been archived, state how to access that archived data.
Archive Software	Explain where the old software is stored. If the old software has been archived, state how to access that archived software.

Appendix A - Templates

Following are templates for the Migration Plan, Migration Plan Approval Memo, Decommission Plan, Decommission Plan Approval Memo, Certificate of Decommissioning, Post Decommission report, and Decommissioning Criteria.

Migration Plan Template

Fill in the following information for each system being decommissioned.

Note: This form contains multiple sections with fields that are identified by square brackets "[ ]" in which information for each section can be provided. Please provide all necessary information for each section to complete the form.

Date:	[EnterDate]		
Project Manager Information			
Name:	[EnterName]	**Email address:**	[EnterEmail]
Agency:	[EnterAgency]	**Telephone:**	[EnterTelephone]
System Information			
Legacy System Name:	[EnterSystemName]	**Legacy System DEAR / CSAM ID:**	[EnterSystemID]

Legacy System Overview

Include an overview of the system undergoing migration. Provide a brief overview of the functions the system is currently supporting (mapped to the BRM). Also include the type of data maintained in the legacy system (mapped to the DRM). The BRM and DRM mappings should match those found in the DEAR or CSAM.

[EnterLegacySystemOverview]

Target System DEAR / CSAM ID:	[EnterTargetSystemID]

Target System Overview

Provide an overview of the target system, including a brief overview of the functions from the legacy system that the target system will be supporting (mapped to the BRM) along with the type of data maintained in the legacy system that will be maintained in the target system (mapped to the DRM). The BRM and DRM mappings should match those found in the DEAR/CSAM.

[EnterTargetSystemOverview]

Migration Overview

Describe the structure and major components of the legacy system and designate which system components will and will not be migrated. The legacy system structure should match the system hierarchy found in DEAR/CSAM and each system component within DEAR/CSAM should be identified in this section as to whether it will be migrated or not. If the migration process will be organized into discrete phases, each of the BRM, SRM, DRM, and TRM mappings in DEAR/CSAM should be listed with details as to where and when they will be migrated.

[EnterMigrationOverview]

Migration Requirements

Include any special requirements for the migration, including specific detail as to what is required to be migrated, who is setting each requirement, and whether any of the requirements will be delayed beyond the original migration schedule.

[EnterMigrationRequirements]

Hardware Migration Overview

Include a detailed description of the migration from legacy system hardware. Describe the legacy hardware that will no longer be used and the new (target) hardware to which the system is being migrated. The legacy hardware should be mapped to the legacy system in DEAR and the target hardware should be mapped to the target system in DEAR/CSAM.	
[EnterHardwareMigrationOverview]	
Are Hardware Components Mapped in DEAR/CSAM? (Yes/No)	[Enter(Y/N)]
Software Migration Overview	
Include a detailed description of the migration from legacy system hardware. Describe the legacy hardware that will no longer be used and the new (target) hardware to which the system is being migrated. The legacy hardware should be mapped to the legacy system in DEAR/CSAM and the target hardware should be mapped to the target system in DEAR/CSAM.	
[EnterSoftwareMigrationOverview]	
Are Software Components Mapped in DEAR/CSAM? (Y/N)	[Enter(Yes/No)]
Data Migration Overview	
Describe the data migration strategy, data quality assurance, and the data migration controls. All data mapped to the legacy system in DEAR/CSAM should be listed and accounted for in this section in terms of where and when it will be migrated. The target system in DEAR/CSAM should have the data mappings from the DRM populated. *All records should be managed following BLM policies on records management, and that all electronic records should be managed following the National Archives regulations, NARA Records management Guidance and Regulations, subchapter B, Record Management, Part 1234 (last amended on 2/21/06)*	
[EnterDataMigrationOverview]	
Are Data Components Mapped in DEAR/CSAM? (Y/N)	[Enter(Yes/No)]
Security Overview	
Describe the system security and access rights associated with the legacy system. Specifically, any security features associated with the system, its network configuration, its use authorization capabilities, data level security considerations, and any other security features should be described as well as how those security features will be accommodated or modified by the new (target) system.	
[EnterSecurityOverview]	
Impact to Interfaces	
Include a description of the legacy interfaces to other systems that will be affected by the migration. The legacy system to feeder system interfaces should be detailed in DEAR/CSAM and the target system to feeder system interfaces should also be detailed in DEAR/CSAM.	
[EnterInterfaceImpacts]	
Are Interfaces Detailed in DEAR/CSAM? (Y/N)	[Enter(Yes/No)]
Test Plan:	
Describe the testing that will be conducted to ensure that all migration activities are successful. At a minimum, this section should include details regarding who will perform the testing, the test cases that will be performed, and how the results of the testing will be tracked and reported.	
[EnterTestPlanDetails]	
Migration Risks	

Describe the testing that will be conducted to ensure that all migration activities are successful. At a minimum, this section should include details regarding who will perform the testing, the test cases that will be performed, and how the results of the testing will be tracked and reported.
[EnterMigrationRisks]

Migration Schedule	
Migration Schedule File Name:	[EnterFileName]
Migration Schedule Location:	[EnterFileLocation]

Migration Resources
Provide a description of the resources necessary to perform the migration. Required hardware, software, people, and facilities resources not currently available should be highlighted in this section. Additionally, an approach for obtaining all currently unavailable resources should be detailed.
[EnterMigrationResourceDetails]

Migration Plan Approval Memo Template

Date: xx/xx/xxxx

To: File

Subject: Approval of Migration Plan for Legacy System <name> to Receiving/Target System <name>

We, the undersigned, certify that the migration plan for the legacy system, <name>, to the target system, <name>, has been developed in accordance with applicable Bureau of Land Management (BLM) directives. We acknowledge that, by signing this memorandum, we approve commencing activities associated with migration of the legacy system, <name>, system as described in the system migration plan.

_____	_____
ADIRM (Legacy System)	ADIRM (Receiving/Target System)
_____	_____
Chief Information Security Officer (Legacy System)	Chief Information Security Officer (Receiving/Target System)
_____	_____
Privacy Officer (Legacy System)	Privacy Officer (Receiving/Target System)
_____	_____
Records Officer (Legacy System)	Records Officer (Receiving/Target System)
_____	_____
Chief Architect (Legacy System)	Chief Architect (Receiving/Target System)
_____	_____
System Owner for Legacy System	System Owner for Receiving/Target System

_____

Project Manager Responsible for the Decommissioning

Certificate of Migration Template

Date: xx/xx/xxxx

We, the undersigned, certify that the migration of legacy system, <name>, to target system, <name>, has been successfully completed. We certify that: business functions/processes are adequately supported in the receiving/target system, all data has been adequately migrated per the migration plan, the updates have been made to the system inventory source of record in Bureau of Land Management (BLM) Cyber Security Assessment Management (CSAM), and requirements for records management, security and privacy, and quality assurance testing have been satisfied. We acknowledge that, by signing this certificate of migration, the activities associated with officially decommissioning legacy system, <name>, may now commence.

_____	_____
ADIRM (Legacy System)	ADIRM (Receiving/Target System)
_____	_____
Chief Information Security Officer (Legacy System)	Chief Information Security Officer (Receiving/Target System)
_____	_____
Privacy Officer (Legacy System)	Privacy Officer (Receiving/Target System)
_____	_____
Records Officer (Legacy System)	Records Officer (Receiving/Target System)
_____	_____
Chief Architect (Legacy System)	Chief Architect (Receiving/Target System)
_____	_____
System Owner for Legacy System	System Owner for Receiving/Target System

_____

Project Manager Responsible for the Migration

Decommission Plan Template

Fill in the following information for each system being decommissioned.

Note: This form contains multiple sections with fields that are identified by square brackets "[ ]" in which information for each section can be provided. Please provide all necessary information for each section to complete the form.

Date:	[EnterDate]		
Project Manager Information			
Name:	[EnterName]	**Email address:**	[EnterEmail]
Agency:	[EnterAgency]	**Telephone:**	[EnterTelephone]
System Information			
Legacy System Name:	[EnterSystemName]	**Legacy System DEAR/CSAM ID:**	[EnterSystemID]
Legacy System Decommission Date:	[EnterDate]	**Date of Migration Certificate:**	[EnterDate]

Software Archive Overview

Describe the plan for archiving the software library files and related documentation in the system being decommissioned. Include all necessary software and formats as would be required in the event that the system must be re-initiated. Software associated with decommissioned systems should be archived in accordance with records disposition schedules.

[EnterSoftwareArchiveOverview]

Documentation Archive Overview

Describe the plan for archiving the hardcopy, softcopy and user documentation for the systems being decommissioned. Include all documentation and formats that would be necessary in the event that the system is to be re-initiated. Software associated with decommissioned systems should be archived in accordance with records disposition schedules.

[EnterDocumentationArchiveOverview]

Hardware Disposition Overview

Describe the plan for disposing of hardware that was used exclusively by the decommissioned system. It is recommended that the hardware disposition leverage the Environmental Protection Agency's (EPA) Ecycling program. Ecycling is designed to prevent hazardous substances inside these items from entering landfills.

[EnterHardwareDispositionOverview]

Data Archive Overview

Describe the plan for archiving data files and related documentation in the system being decommissioned. This section should outline which data has been migrated, which data will be archived, and in which format. All electronic records should be managed following the National Archives regulations, NARA Records management Guidance and Regulations, subchapter B, Record Management, Part 1234 (last amended on 2/21/06).

[EnterDataArchiveOverview]

Security Overview

Provide a description of the system security and access rights associated with the legacy system. The intent of this section is to provide in the decommission guide the necessary security information so that the system, if needed, could be reconstituted with the same security considerations.
[EnterSecurityOverview]
Decommission Risks
Describe the major risk factors in the decommission effort and strategies for their control or reduction. Descriptions of the risk factors that could affect the decommission feasibility, the decommission schedule, or costs should be included.
[EnterDecommissionRisks]
Decommission Schedule

Decommission Schedule File Name:	[EnterFileName]
Decommission Schedule Location:	[EnterFileLocation]

Decommission Resources
Describe the resources necessary to perform the decommission activities. Any required hardware, software, people, and facilities resources not currently available should be highlighted in this section. An approach for obtaining all currently unavailable resources should be detailed in this section.
[EnterDecommissionResourceDetails]

Decommission Plan Approval Memo Template

Date: xx/xx/xxxx

To: File

Subject: Approval of Decommission Plan for _____ System

We, the undersigned, certify that the decommission plan for the <name> system has been developed in accordance with applicable Bureau of Land Management (BLM) directives. We acknowledge that, by signing this memorandum, we approve the commencement of activities associated with decommissioning of the <name> system as described in the system decommission plan.

_____

ADIRM

_____

Chief Information Security Officer

_____

Privacy Officer

_____

Records Officer

_____

Chief Architect

_____

Authorizing Official

_____

System Owner for Legacy System

_____

Project Manager Responsible for the Decommissioning

Certificate of Decommissioning Template

Date: xx/xx/xxxx

We, the undersigned, certify that the decommissioning of system <*name*> has been successfully completed, the updates have been made to the system inventory source of record in Bureau of Land Management (BLM) Cyber Security Assessment Management (CSAM), and that data, software, and documentation have been archived in accordance with BLM directives.

<Include a summary statement of the impacts to the enterprise security posture caused by the decommissioning of the system, and identify the rationale for changes to the certification and accreditation (C&A) boundaries that are impacted by the decommissioning of the system.>

We acknowledge that, by signing this decommissioning certification, activities associated with decommissioning system <*name*> are now complete, and the system will be removed from the BLM IT portfolio.

_____

ADIRM

_____

Chief Information Security Officer

_____

Privacy Officer

_____

Records Officer

_____

Chief Architect

_____

System Owner for Legacy System

_____

Authorizing Official

_____

Project Manager Responsible for the Decommissioning

Post - Decommission Review Report Template

Fill in the following information for each system being decommissioned

Note: This form contains multiple sections with fields that are identified by square brackets "[ ]" in which information for each section can be provided. Please provide all necessary information for each section to complete the form.

Date:	[EnterDate]		
Project Manager Information			
Name:	[EnterName]	**Email address:**	[EnterEmail]
Agency:	[EnterAgency]	**Telephone:**	[EnterTelephone]
System Information			
Legacy System Name:	[EnterSystemName]	**Legacy System DEAR/CSAM ID:**	[EnterSystemID]
Legacy System Decommission Date:	[EnterDate]	**Date of Decommission Certificate:**	[EnterDate]

Lessons Learned: Data

This section should include a description of what happened to the data from the old system. Explain any problems or mishaps that might have occurred during decommissioning of the data and things for others to consider in future decommission efforts.

[EnterLessonsLearned]

Lessons Learned: Software

This section should include a description of what happened to the software from the old system. Explain any problems or mishaps that might have occurred during the decommissioning of the software and things for others to consider in future decommission efforts.

[EnterSoftwareLessonsLearned]

Lessons Learned: Hardware

This section should include a description of what happened to the hardware from the old system. Explain any problems or mishaps that might have occurred during decommissioning of the hardware and things for others to consider in future decommission efforts.

[EnterHardwareLessonsLearned]

Archive Data

This section should include an explanation for where the old data is stored. If the old data was incorporated into a new system, it should be stated here. If some of the old data has been archived, state how to access that archived data.

[EnterArchivedDataDetails]

Archive Software

This section should include an explanation for where the old software is stored. If the old software has been archived, state how to access that archived software.

[EnterLessonsArchivedSoftwareDetails]

Archive Hardware
This section should include an explanation for where the old hardware is located. If the hardware has been excessed, provide the date it was excessed. If the hardware is being reused for another function, provide some explanation for where and how it is being reused.
[EnterArchivedHardwareDetails]

Decommissioning Criteria

The decommissioning criteria are available in the "Document Library" section of the BLM CPIC website at: http://teamspace/sites-wo/ls-irm/InvestmentManagement/CPIC/default.aspx.

Appendix B - Glossary

Term	Description
ADS	Authoritative Data Source
BRM	Business Reference Model
C&A	Certification and Accreditation A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to accept explicitly the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
CCM	Change Control and Management
Migration	The activities required to move functionality and data from a legacy system to a receiving/target system
Certificate of migration	A certificate acknowledging that all activities in the migration plan have been successfully completed
Migration Plan	A document that describes the strategies and activities involved in migrating from the existing system to a receiving/target system, hardware, or software environment
CSAM	Cyber Security Assessment Management
DEAR	Department Enterprise Architecture Repository, the system of record for the BLM system inventory
Decommissioning	Activities that result in the termination of an IT system's operations
Decommission Certification	A certificate acknowledging that all activities in the decommissioning plan have been completed
Decommission Plan	A document that describes how the decommissioning of the system will be conducted including the software components, data migration, disposition of equipment, and archiving of life-cycle products
BLM	Bureau of Land Management
DRM	Data Reference Model
EA	Enterprise Architecture
Ecycling Program	The EPA offers Ecycling as a service to federal agencies for recycling electronics and assets in order to help agencies recycle or properly dispose of computers and other electronic equipment. Ecycling is designed to prevent hazardous substances inside these items from entering landfills.

Term	Description
EPA	Environmental Protection Agency
Information Resources	Information and related resources, such as personnel, equipment, funds and information technology
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Information Technology	IT. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that: 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
MS Project	Microsoft Project, a project management software tool
NARA	National Archives and Records Administration
NIST	National Institute for Standards and Technology
OCIO	Office of the Chief Information Officer
Post-Decommission Review	The documentation of lessons learned from the decommissioning activities
SLA	Service Level Agreement
SRM	System Component Reference Model
TRM	Technical Reference Model

References

DOI Methodology for Business Transformation (MBT):
http://www.doi.gov/ocio/architecture/mbt/guidance.htm

DOI guidance for maintaining the DOI Enterprise Architecture Repository (DEAR):
http://www.doi.gov/ocio/architecture/guidance/dearguidance.htm

DOI Technical Reference Model:
http://www.doi.gov/ocio/architecture/fea.htm#trm

BLM Records Management Program:
http://web.blm.gov/internal/wo-500/records/records.html

NARA Records Management Guidance and Regulations, subchapter B, Record Management, Part 1234 (last amended on 2/21/06) -- Electronic Records Management:
http://www.archives.gov/about/regulations/part-1234.html

NARA Frequently Asked Questions (FAQs) about Selecting Sustainable Formats for Electronic Records: http://www.archives.gov/records-mgmt/initiatives/sustainable-faq.html

National Institute of Standards and Technology (NIST), Computer Security Division, Computer Security Resource Center:
http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf.

Information Technology (IT) Security Policy, Bureau of Land Management:
http://web.blm.gov/internal/wo-500/security/Security.html

United States Code 40, Section 11101, Information Technology Management, January 2006:
http://uscode.house.gov/download/pls/40C111.txt

OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000:
http://www.whitehouse.gov/omb/circulars_a130_a130trans4