



Decommission Phase Procedures

Version 1.1

June 2011



Version History

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Description of Change
1.0	Chris Niedermayer	December 20, 2010			Final Version 1.0
1.1	Chris Niedermayer	June 27, 2011			Updates to styles and quality assurance review



Contents

1.	Decommission Phase Procedures	1
1.1	Decommission Phase Description	2
1.1.1	High-Level Task Process Flow.....	2
1.1.2	Entry Criteria/Input.....	3
1.1.3	Control Gate Review Criteria	3
1.1.4	Tasks.....	3
1.2	Decommission Phase Task Description.....	4
T7-1	Develop a Decommission Plan.....	4
T7-2	Remove User Access and Terminate Operations.....	6
T7-3	Archive/Migrate Data Records.....	8
T7-4	Archive Software Components and Documentation	10
T7-5	Reallocate or Dispose of Hardware.....	12
T7-6	Update IAS, CSAM, and EBITS	13
T7-7	Develop Deletion of System of Records Notice	15
T7-8	Create Post-Decommission Report	16

1. Decommission Phase Procedures

The Department of Housing and Urban Development’s (HUD) Project Planning and Management (PPM) Life Cycle is the rigorous application of sound investment, project management principles, and best practices for organizing and managing Information Technology (IT) projects. As a component of HUD’s overarching Information Technology Management (ITM) Framework it provides the context for the HUD IT governance process and describes the interdependencies between project management, investment management, and capital planning components.

The PPM Life Cycle covers all aspects of a project from the initial development of an idea through to its decommissioning. Because there is wide variance in the methods, techniques and tools needed to support an IT project, the PPM Life Cycle is flexible and can be tailored to address the needs and requirements of each individual project regardless of its size. It aims to capture the minimum level of detail necessary to ensure project success. Each project, working in conjunction with the Office of the Chief Information Officer (OCIO), will capture decisions around PPM Life Cycle tailoring in the *Project Process Agreement* (PPA), which documents the reasons for using, combining, or skipping specific artifacts applicable to the project.

The PPM Life Cycle applies to all HUD IT projects, including but not limited to:

- New projects
- Major enhancements to existing projects
- Projects associated with operations and maintenance investments
- High-priority, fast-track IT projects
- New Commercial-off-the-Shelf (COTS) product acquisitions

There are seven major phases of the PPM Life Cycle; artifacts have been created for each phase. These artifacts are interrelated, either rolling up other artifacts, or building upon a concept to define a lower level of detail.

This document addresses the processes and related procedures for the Decommission Phase, the seventh phase in the PPM Life Cycle.



Figure 1 - The Decommission Phase Relative to the Entire PPM Life Cycle

The purpose of this document is to:

- Provide a detailed description of the phase
- Identify the tasks and activities that take place during the phase
- Give guidance and templates on completing the tasks and activities required to exit the phase
- Detail the roles and responsibilities associated with completing each of the tasks and activities for this phase

1.1 Decommission Phase Description

Inevitably, changes in business requirements and technology will necessitate the retirement of IT solutions. The purpose of the Decommission Phase is to retire the solution when operational analysis indicates that the solution no longer provides sufficient business value and/or is no longer cost-effective to operate. The outcome of the Decommission Phase is the deliberate and systematic decommissioning of the solution with appropriate consideration of data archiving and security, migration of data or functionality to new solution(s), and incorporation of lessons learned over the solution’s life cycle.

The Decommission Phase represents the end of the solution’s life cycle. A *Decommission Plan* is prepared and executed to address all facets of archiving, transferring, and disposing of the solution’s software and hardware components. Particular emphasis is given to proper preservation of the data processed by the solution so that it is effectively migrated to another solution or archived in accordance with applicable records management regulations and policies for potential future access.

The decommission activities are planned and executed with input from several stakeholder groups including the solution development team, operations and maintenance, records management, legal counsel, security, enterprise architecture, and interfacing systems.

1.1.1 High-Level Task Process Flow

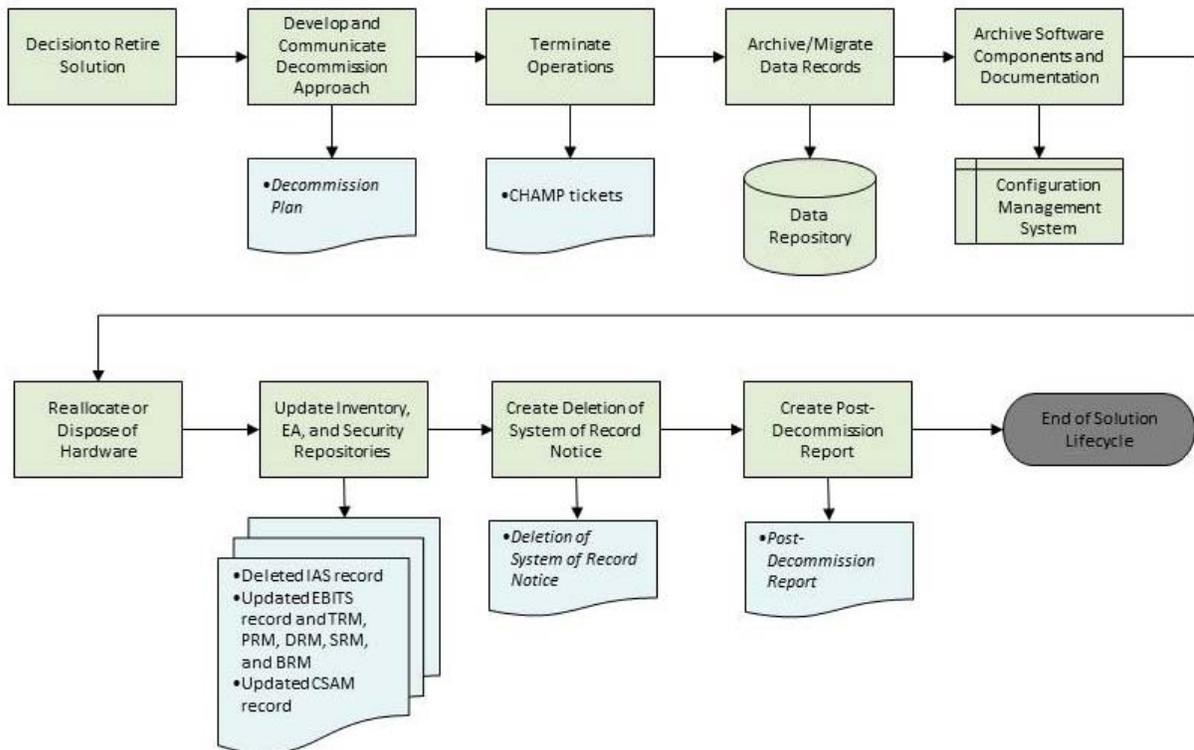


Figure 2 - High-Level Decommission Phase Process Flow



1.1.2 Entry Criteria/Input

Before the Decommission Phase can begin, the operational solution must be selected for retirement. A solution typically is selected for retirement if the annual operational analysis reveals that it does not meet a current business need, is redundant, and/or technologically obsolete.

1.1.3 Control Gate Review Criteria

In order to complete the Decommission Phase control gate, the project must receive approval of the Decommission Phase package. The Decommission Phase package consists of:

- *Decommission Plan*
- *Post Decommission Report*
- *Deletion of System of Records Notice* (optional)

1.1.4 Tasks

The following tasks take place in the Decommission Phase:

- T7-1 Develop a *Decommission Plan*
- T7-2 Remove User Access and Terminate Operations
- T7-3 Archive/Migrate Data Records
- T7-4 Archive Software Components and Documentation
- T7-5 Reallocate or Dispose of Hardware
- T7-6 Update IAS, CSAM, and EBITS
- T7-7 Develop *Deletion of System of Records Notice*
- T7-8 Create the *Post Decommission Report*



1.2 Decommission Phase Task Descriptions

T7-1 Develop a Decommission Plan

What Happens?

The strategy for decommissioning the solution is finalized and detailed in the *Decommission Plan*.

Who Does What?

The business and IT project managers (PMs), IT security specialist, enterprise architecture (EA) representative, records manager, operations manager, database administrator, and other stakeholders develop a *Decommission Plan* that documents the activities and schedule to shut down the IT solution.

What Comes in?

- *Annual Operational Analysis Report* (with recommended retirement strategy)

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- *Decommission Plan* template, instructions, and checklist

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
<i>Decommission Plan</i>	Responsible	IT PM	X				
	Accountable	Business PM					
	Consulted	IT security specialist, IPT Database administrator, Records manager, Operations project team					
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-1.1 Gather Stakeholder Input – The IT and business project managers communicate with the stakeholder groups that most use the solution. They determine the current usage of the data, functionality of the solution, and nature of the usage (mission critical, very useful, marginally useful, or optional). In addition, the team seeks to identify any technical interdependencies with other systems that may need to be addressed and determines if there are other solutions that can absorb any of the solution’s data or functionality that is still heavily used.



The team coordinates with internal and external organizations that consume any data or services from the retiring solution or provide data or services to the solution. They identify any *Memoranda of Understanding* or other interface agreements that will need to be closed out or modified.

T7-1.2 Develop Retirement Approach – The team determines the scope of the retirement effort; establishes the approach for decommissioning and disposing of the solution’s hardware and software components, data, and documentation; identifies key retirement milestones; and, charts a detailed schedule of tasks.

T7-1.3 Communicate Decision to Stakeholders – The team drafts an initial communication for distribution to the stakeholder community notifying them of the decision to terminate operation of the solution. If different potential audiences are likely to have different priorities with regard to the solution’s retirement, the communication is customized to address the unique sensitivities of the different audiences. The communication is reviewed and approved by appropriate management (including the solution owner) before it is sent out. At a minimum, the contents of this initial communication includes:

- The rationale for disposing of the solution
- The plan for transitioning any data or functionality that will be retained
- The tentative timeline for disposition

T7-1.4 Prepare Decommission Plan – The team uses the guidelines laid out in the *Decommission Plan* template, checklist, and instructions to develop a draft *Decommission Plan* that addresses how the various components of the solution will be handled at the completion of operations, including software, data, hardware, communications, and documentation. The plan also notes any provisions for future access to the solution’s components particularly the data. The plan is forwarded to appropriate management personnel and stakeholders for review and approval.

T7-1.5 Communicate Schedule to Stakeholders – The team prepares another communication that is customized to address the different stakeholder audiences identified earlier. The purpose is to communicate the details of the plan. At a minimum, it includes the planned schedule for the solution decommissioning and any known outages that will occur during the disposition.



T7-2 Remove User Access and Terminate Operations

What Happens?

All user access to the solution is blocked and business processes running on the solution are shut down.

Who Does What?

The IT, business, and operations managers coordinate with the HUD Information Technology Service (HITS) team to revoke all users’ access to the solution and shut down all processes running on the solution.

What Comes in?

- Approved *Decommission Plan*

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- Operations and security guidelines

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
CHAMP tickets	Responsible	Operations project team	X				
	Accountable	Business PM					
	Consulted	IT PM Operations manager					
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-2.1 Eliminate Access to Solution – The business PM works with the IT PM and operations manager, as well as the HITS team, to create and process Centralized HUD Account Management Process (CHAMP) tickets to revoke all user access rights except those required for the team members participating in the decommissioning activities. This is done in accordance with the schedule detailed in the *Decommission Plan* and communicated to the user community. If the solution being retired is part of an integrated system or is accessed via a single sign-on process, the team exercises caution to ensure that the users’ access to other remaining solutions is not adversely affected. If the solution is being replaced, the team coordinates with the managers of the replacement solution to assure timely transfer of users’ access.

T7-2.2 Shut-Down Operations – The business manager works with the IT and operations managers, as well as the HITS team, to cease all processes running on the solution. This includes any data interchanges with interfacing systems/organizations, nightly batch jobs, or other routine



processes. The team posts a notice on appropriate HUD intranet and internet sites alerting stakeholders that the solution is no longer operational.



T7-3 Archive/Migrate Data Records

What Happens?

Data is transferred to another solution, if applicable. Data is archived in accordance with the data retention plan outlined in the *Decommission Plan*.

Who Does What?

The IT project manager, database administrator, IT security specialist, and records manager coordinate the transfer and archiving of the solution’s data records.

What Comes in?

- Approved *Decommission Plan* with data retention plan and applicable migration approach

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- HUD Records management guidelines
- Federal records management requirements (<http://www.archives.gov/records-mgmt/policy/> and <http://www.archives.gov/about/laws/>)

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
Archived Records	Responsible	Records manager					
	Accountable	Business PM					
	Consulted	Database administrator, IT security specialist, Operations project team		X			
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-3.1 Archive Data – The IT manager and database administrator coordinate with the HITS team to archive the data onto permanent storage media and store the media in a location designated by the *Decommission Plan*. The archival method and storage media will vary depending upon the solution. However, regardless of the method and media, the team ensures that information is retained in a usable format with attention paid to the retrieval method that will be used in the future to access the data. The security specialist and database administrator make certain that any necessary encryption is applied for long-term storage and that sensitive data that does not need to be retained is successfully and securely destroyed. The records manager and



representatives from the legal department provide directions regarding the legal and organizational requirements for records retention.

To preserve the integrity of the historical data, the team ensures that the archival activities:

- Preserve the business context of the archived data
- Provide access capabilities that ensure fast and easy retrieval for research and reporting, as well as audits and e-discovery requests
- Implement appropriate storage strategies, based on business value and access requirements, to lower costs throughout retention periods

T7-3.2 Migrate/Transfer Data – If data is being migrated to another solution, the database administrator works with the representatives of the other solution(s) to develop any required extract, transform, and load (ETL) logic to achieve a smooth transfer of data from the current solution to those solutions.

T7-3.3 Sanitize Media – The database administrator and IT security specialist determine the purging technique that most accurately matches the level of security that the data requires. They ensure that the data is irretrievable from the retired storage media. The National Institute of Standards and Technology (NIST) publication, “Guidelines for Media Sanitization” ([NIST Special Publication 800-88](#)), defines the removal of information from a storage medium (such as a hard disk or tape) as sanitization. Different categories of sanitization can provide different levels of protection for data. Sanitization methods include the following:

- Overwriting uses special software to overwrite every bit in every sector of memory
- Degaussing is more destructive and involves physically destroying the magnetic image
- Destruction is the most reliable technique since the media is taken to an approved facility for incineration or application of an abrasive substance



T7-4 Archive Software Components and Documentation

What Happens?

All software components are stored in the configuration management system with the appropriate labels. Solution documents are also archived.

Who Does What?

The IT PM, configuration manager, and other stakeholders ensure that all software components are stored and labeled in the configuration management system. The team also stores documents in the configuration management system or other appropriate location.

What Comes in?

- Approved *Decommission Plan* with software component retention/disposition approach
- *Configuration Management Plan*

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- HUD configuration management guidelines

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
Archived software components and documents	Responsible	IT PM					
	Accountable	Business PM					
	Consulted	Configuration manager, Operations project team				X	
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-4.1 Archive or Transfer Software Components – The decommission team ensures that all software components are stored, appropriately labeled, and version controlled in the configuration management system. They record the applied version label in the *Decommission Plan*. If necessary, the team copies software onto permanent storage media and store the media in a location designated in *Decommission Plan*. (Software to be stored may include communications and systems software as well as application code.) If any of the software components is to be reused in another solution, the IT project manager provides the team(s) with the location and version label of the components.



T7-4.2 Archive Lifecycle Deliverables – The IT PM, business PM, and the configuration manager store artifacts and other documentation (including manuals received from vendors), in archive locations identified in the *Decommission Plan*. Ideally, the documentation is stored, appropriately labeled, and version controlled in the same configuration management system as the software components.



T7-5 Reallocate or Dispose of Hardware

What Happens?

Hardware and other equipment used exclusively by this solution is either salvaged and reallocated for use by other solutions or discarded in accordance with Federal and HUD guidelines.

Who Does What?

The server manager, telecommunications manager, network manager, and other stakeholders identify the excess hardware components and reallocate them to other solutions or dispose of them.

What Comes in?

- Hardware components from decommissioned solution

What Controls Need to be Used?

- HITS contract terms
- Federal and HUD IT asset disposition guidelines

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
Salvaged Hardware	Responsible	IT PM					X
	Accountable	Business PM					
	Consulted	Configuration manager, Operations project team					
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-5.1 Reallocate or Discard Hardware – The IT PM, network manager, and server manager collaborate with the HITS team to ensure that all excess hardware is reallocated to other solution(s), recycled, destroyed, or otherwise disposed of in accordance with the terms of the HITS contract that covers HUD infrastructure.



T7-6 Update IAS, CSAM, and EBITS

What Happens?

The retired solution is removed from HUD’s Inventory of Automated Systems (IAS). The solution’s record is updated in Cyber Security and Management System (CSAM), Enterprise Business Information Transformation System (EBITS), and any other applicable enterprise architecture-related document(s).

Who Does What?

The business and IT PMs coordinate the removal of the solution from IAS.

The enterprise architecture representative updates the EBITS record(s) and the HUD Technical, Service, Data, Business and Performance Reference Models.

The IT security specialist updates the solution’s record in CSAM.

What Comes in?

- Decommission notice and results
- Existing IAS, CSAM, and EBITS records

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- IAS and CSAM guidelines
- Enterprise architecture guidelines

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
Deleted IAS record	Responsible	IT Security specialist					
	Accountable	Business PM				X	
	Consulted	IT PM					
	Informed	TRC/CCC/EIB					
Updated CSAM record	Responsible	IT Security specialist					
	Accountable	Business PM				X	
	Consulted	IT PM					
	Informed	TRC/CCC/EIB					
Updated EBITS record and TRM/DRM/BRM/SRM/PRM	Responsible	EA representative					
	Accountable	Business PM				X	
	Consulted	IT PM					
	Informed	TRC/CCC/EIB					



Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

- T7-6.1 Update IAS** – The business PM ensures that the solution’s record is removed from HUD’s Inventory of Automated Systems.
- T7-6.2 Update CSAM** – The IT security specialist updates the solution’s security and privacy records in CSAM to indicate that the solution has been decommissioned.
- T7-6.3 Update Enterprise Architecture Information** – The EA representative makes sure that the solution is marked as decommissioned in EBITS and that any dependencies or relationships to the decommissioned solution are redirected or similarly decommissioned if no replacement capability exists. The EA representative performs impact analysis to determine what changes need to be made to the architecture as a result of the solution’s decommissioning. The EA representative updates the Technical Reference Model, Business Reference Model, Data Reference Model, Service Reference Model, and Performance Reference Model as necessary.



T7-7 Develop Deletion of System of Records Notice

What Happens?

A Deletion of *System of Records Notice* is prepared in accordance with the requirements of the Privacy Act of 1974. This task only applies to those systems with a *System of Records Notice* (SORN) published in the Federal Register. If the records retention schedule requires that the system records be retained for a specified period after the system no longer exists, the SORN may not be deleted until after the records retention schedule has been satisfied.

Who Does What?

The business project manager coordinates with the Office of Public Affairs representative to prepare a Deletion of *Systems Records Notice* for publication in the Federal Register.

What Comes in?

- *System of Record Notice*

What Controls Need to be Used?

The team uses the controls listed below to create the relevant artifacts or complete the task activities:

- Federal Register publication guidelines

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
Deletion of <i>System of Records Notice</i>	Responsible	IT Security specialist	X				
	Accountable	Business PM					
	Consulted	Office of Public Affairs					
	Informed	Investment owner					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-7.1 Develop Deletion of System of Records Notice – The business PM works with the Office of Public Affairs to prepare the Deletion of *System of Records Notice* in accordance with the requirements of the Privacy Act and Federal Register publication guidelines. A deletion notice is required whenever a system is discontinued, integrated into another system, or determined to be no longer subject to the Privacy Act. The notice of deletion includes:

- The system identification number/code and name
- The reason for the deleting the SORN from the Federal Register
- If the system is eliminated through replacement or integration, an identification of the successor system or systems
- The effective date of the deletion



T7-8 Create Post-Decommission Report

What Happens?

A *Post-Decommission Report* is generated that provides the official record of the decommission activities. This document also describes the lessons learned for future decommissioning efforts.

Who Does What?

The IT and business PMs complete the *Post Decommission Report*, with input from other stakeholders and participants in the decommission activities.

What Comes in?

- *Decommission Plan*
- Feedback from stakeholders and participants in the decommission activities
- Output from lessons learned meeting(s)

What Controls Need to be Used?

- *Post Decommission Report* template, instructions and checklist

What is Produced?

Work Products	Responsibilities		Must Create	Should Create	Should Update	Must Update	Must Complete
<i>Post-Decommission Report</i>	Responsible	Business PM	X				
	Accountable	Investment owner					
	Consulted	IT PM, Server manager, Telecommunications manager, Network manager, Configuration manager					
	Informed	TRC/CCC/EIB					

Detailed Tasks:

The following defines the detailed sub-tasks that take place within this task:

T7-8.1 Complete Post-Decommission Report – The business PM creates the *Post Decommission Report* that documents the tasks performed to dispose of the solution. It details the *Lessons Learned* from the decommission process and describes the location of all data, software components, and documentation that were archived. If data, software components, or hardware and peripherals were migrated or integrated into other solutions, the report specifies the disposition details. The business PM collaborates with all stakeholders that participated in the decommission activities and uses the *Post Decommission Report* template, instructions, and checklist as guidelines in creating the report.