E-AUTHENTICATION ROLL-OUT

FOR LOGICAL ACCESS

RELEASE 1.0

DEPLOYMENT PLAN

MAY 21, 2004

Prepared for:

The Bureau of Land Management
WO-850
Department of the Interior

Prepared by:

Timothy Foley

Under Consulting Agreement Number 359

Approval

Submitted By:

T Foley Date: 5/21/04

Name: Timothy Foley

Title: e-Authentication Project Manager, BLM contract

Approved By:

Date: 5/21/04

Name: Bob Donelson,

Title: Project Sponsor,
DOI Representative to OMB for Electronic Signature
Senior Property Management Specialist, BLM WO-850

Concurred by:

Lawrence E Benna Date: 6/23/04

Name: Larry Benna

Title: Chief Financial Officer, BLM

Concurred by:

Acting DIAD Date: 6/25/04

Name: Ronnie Levine

Title: Chief Information Officer, BLM

E-AUTHENTICATION LOGICAL ACCESS DOCUMENT 1.0
THE DEPLOYMENT PLAN

CONTENTS

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Scope 1

1.3 Overview of Deployment Strategy 1

1.3.1 Relationship to other activities 1

1.3.2 Limitations 1

1.3.3 Assumptions 1

2 REFERENCED DOCUMENTS 2

3 MANAGEMENT 3

3.1 The Organization 4

3.2 Authorities 4

3.3 Roles and Responsibilities 4

3.4 Applicable policies, directives, and procedures 4

4 ACTIVITIES TO BE PERFORMED 5

4.1 IT Security Management 5

4.2 Change Management 5

4.2.1 Inventory Management 5

4.2.2 Acquiring Additional Inventory 6

4.3 Records Management 7

4.4 Quality Assurance and Reviews 7

4.5 Training 8

5 DEPLOYMENT SCHEDULE 9

6 RESOURCES **9**

7 PLAN MAINTENANCE **10**

7.1 List of Acronyms and Abbreviations 10

7.2 Volume Glossary 10

7.3 Additional Sections (4.3 thru 4.X) 10

8 ILLUSTRATIONS, TABLES, AND FIGURES **10**

Appendices

APPENDIX A: INVENTORY **A-1**

APPENDIX B: KEYBOARD READER DISTRIBUTION **B-2**

APPENDIX C: PCMCIA READER DISTRIBUTION **C-1**

APPENDIX D: USB STAND ALONE READER DISTRIBUTION **D-2**

APPENDIX E: GENERAL RECORDS SCHEDULE 24 .... **E-3**

1 INTRODUCTION

1.1 Purpose

This plan sets forth the activities to be accomplished that will ensure successful issuance and use of digital certificates for logon to the Bureau of Land Management (BLM) computer network. State and Center Chief Information Officers (CIO) are to use this plan when planning deployment activities. Each State and Center CIO is required to prepare a Deployment plan based on this parent document and submit it for approval to the Deputy Chief, Information Officer.

1.2 Scope

Although this is a Department of Interior (DOI) system, this plan applies only to the deployment and implementation of the system at BLM facilities and the DOI Office of the Secretary. This plan applies to all Office of the Secretary components and all BLM offices.

1.3 Overview of Deployment Strategy

1.3.1 Relationship to other activities

DOI smart card identity cards are being issued to all employees and certain contractors and volunteers. For individuals approved access to BLM/DOI computer systems, these smart cards will be encoded with the digital certificates used under this project.

1.3.2 Limitations

Funding for the acquisition of required servers and software has been allocated in the FY2003 and 2004 budget. Labor for certificate issuance and network administration is nominal on a per site basis and is expected to be covered in existing office operating budgets. Network logon can not be operational until the publication of a Privacy Act Notice in the Federal Register, expected to occur on about June 20, 2004.

1.3.3 Assumptions

It is assumed that: 1.) Microsoft Office XP has been successfully installed and tested on both the host servers and the PC's using the smart card readers. 2.) All employees will have been issued DOI smart card identity cards prior to the end of the implementation period for this plan. 3.) All BLM offices are using the specification identified in the 2003 and 2004 consolidated buy when replacing desktop and laptop pc's and that those purchases included the keyboard readers specified in the consolidated buy. 4.) That the combination of technology refreshment in 2003 and 2004, supplemented with distribution by the Washington Office of 2,250 keyboard readers, 2,250 USB stand alone readers and 4,500 PCMCIA card readers is sufficient to supply nearly all employees.

2 REFERENCED DOCUMENTS

Title	Status
A Business Case for E-Authentication v.1.1	April 2002
Business Requirements Document v. 1.1	July 2, 2003
MOU between NARA and BLM	#2002-01/RG 049
Logical Access Project Plan	May 11, 2004
Active Directory Schema Change & Software Versions	May 7, 2002
AIMS Enterprise Solution - High Level Architecture v.3	June17, 2003
Version Description Document ActiveCard Gold	December, 2003
Software User's Guide	June 21, 2003
CM Plan	In early draft
Major Application System Security Plan	Draft by Northrup Grumman 12/05/2003 Updated & in review
Interim Authority to Operate	Draft by Northrup Grumman 12/05/2003 Updated & in review
Certification & Accreditation	Awaits installation of security cages
Privacy Impact Assessment	Signed May 21, 2004
Privacy Act Notice	Began surname 4/22/04 At General Law
OARDD	In working draft

3 MANAGEMENT

The logical access component of the e-authentication project is owned by the Department of Interior CIO. The BLM component described in this plan is deployed by the BLM property officer in concert with the BLM CIO's Office. The following are the principals managing functions described in this plan. Each State and Center CIO must document management roles and responsibilities under their jurisdiction.

Project Sponsor
Bob Donelson,
DOI Representative to OMB for Electronic Signature

System Owner
Hord Tipton
Chief Information Officer
U.S. Department of the Interior

System Manager
Scott MacPherson
National Information Resources Management Center Director
Bureau of Land Management

IT Security Manager
Dave Cavallier
IT Security Manager, National IRM Center, BLM

Privacy Act Officer
John Livornese
Privacy Act Officer, BLM

Bureau Enterprise Administrator
Daniel Boss
Idaho State Office, BLM

Project Manager
Tim Foley
Consultant to BLM

Point of Contact
Tiya Darisaw
Property Management

Software Distribution
National Information Resources Management Center (NIRMC)

Bureau of Land Management

3.1 The Organization

DOI Office of the Chief Information Officer – Provides leadership and guidance governing the e-authentication project to ensure consistent deployment and implementation of digital certificates throughout the DOI.

Assistant Director, Business and Fiscal Resources (BLM) – Provides project sponsorship within BLM including the identification of funding and resources needed for successful implementation.

BLM Office of the Chief Information Officer – Provides technical guidance and oversight to ensure security and continuity of computer operations and information relating to the project.

3.2 Authorities

See Section 3 above.

3.3 Roles and Responsibilities

System Manager, NIRMC – Oversees the installation and operation of the certificate server located at the National IRM Center. The System Manager provides guidance and direction to the system administrator of the failover server located at Portland Oregon to ensure consistency in operating procedures and interoperability of the system.

Chief Information Officers, States and Centers – Ensure the secure installation of the certificate issuance hardware and software and the operation Activecard Gold with MS Active Directory at the sites under their responsibility. They also are responsible for assigning a point of contact to coordinate concerns and issues with the project manager.

State and Center IT Security Officers – Ensure secure procedures are in place for the control and issuance of digital certificates including the reporting of compromised certificates.

State and Center IT Security Officers – Ensure secure procedures are in place for the control and issuance of digital certificates including the reporting of compromised certificates.

3.4 Applicable policies, directives, and procedures

Federal Information Security Act (P.L. 104-106), Section 5113.
E-Government Act (P.L. 104-347), Section 203.
DOI OCIO Directive 2004-008 Credentialing Activity Standards and SmartCard Requirements.

4 ACTIVITIES TO BE PERFORMED

4.1 IT Security Management

Personnel authorized to issue certificates, administer the system or access the data contained in the system must receive clearance for medium risk-public trust responsibilities.

4.2 Change Management

The NIRMC Configuration Manger shall provide the needed oversight preparing forms for the System Manager to ensure actions are documented and signed by the approving officials. No change to the hardware or software shall be made unless requested through the National Configuration Control Board as documented in BLM Manual 1268-1. Prior to any changes being made to the hardware and software baseline, they must be approved by the BLM system sponsor during deployment and the DOI system owner after the system is operational. All documents, software, and hardware must be scheduled, released, and tracked.

4.2.1 Inventory Management

This section lists the hardware to be deployed and its configuration and/or specification.

a) The event that created the inventory baseline;
The inventory baseline was created upon approval of the e-Authentication project by the BLM IT Investment Board and the development of a project plan by the project sponsor.
b) The items that are to be managed under the baseline;

A primary enterprise server has been installed at the National IRM Center in Lakewood, Colorado. A failover server has been installed in Portland Oregon. No hardware that is unique to this system is deployed at any other site. The servers at both sites are listed below.

Qty	Server Name/ component	Hardware	Software
Primary Data Centers			
1	Denver AIMS Server - Admin Portal - Content Server - Audit Server	Dual Pentium 4 / Xeon Server 4 GB Ram, RAID 5 Disk Configuration	• Microsoft Windows 2000 • MS-SQL 2000 • IIS 5.0 • All Current Service Packs andPatches
1	Portland Server - Admin Portal - Content Server - Audit Server	Dual Pentium 4 / Xeon Server 4 GB Ram, RAID 5 Disk Configuration	• Microsoft Windows 2000 • MS-SQL 2000 • IIS 5.0 • All Current Patches All Current Service Packs and Patches

Qty	Server Name/ component	Hardware	Software
1	(1) HSM Content Token	Chrysalis Luna RA firmware 3.9 or 3.11	Chrysalis Luna drivers 7.5 or 8.1
	(1) HSM Reader	Chrysalis LunaDock with 2 slots	
1	KMS 1.5	Pentium Class PC – 1 Ghz, 256 MB RAM, 20 GB Hard Drive	Windows 2000 SP6 AIMS Key Management System Gold 2.2
	(1) HSM Principle Token	Chrysalis Luna RA firmware 3.9 or 3.11	Chrysalis Luna drivers 7.5 or 8.1
	(1) HSM Backup Token	Chrysalis Luna RA firmware 3.9 or 3.11	Chrysalis Luna drivers 7.5 or 8.1
	(1) HSM Reader	Chrysalis LunaDock with 2 slots	

c) The procedures used to establish the baseline;

Baseline configuration was established by a working group of BLM specialists led by the system sponsor and with the advice of Cieri Consulting Group Inc.

d) The authority required to approve changes to the approved baseline.

Changes to inventory baseline may only be approved by the BLM system sponsor, Bob Donelson during deployment and implementation. Changes to inventory baseline may only be approved by the system owner, the DOI CIO, after the system is accepted as operational.

Procedures for the storage of hardware, including the physical marking and labeling of items:

All hardware items shall be labeled, listed and accounted for in accordance with BLM property management directives. The hardware is to be housed in a secured space in a manned facility.

Data retention periods and disaster prevention and recovery procedures:

Data retention periods are described in the DOI Privacy Act Notice DOI-15. Disaster prevention and recovery procedures are described in the major application security plan and the contingency plan prepared for this system.

4.2.2 Acquiring Additional Inventory

Additional inventory shall be acquired only with the approval of the State/Center CIO. Funding for replacement of hardware and software components of the system are considered routine operating expense and is the responsibility of the local office.

4.3 Records Management

The National Human Resources Center Records Manager will provide guidance to the project team on disposition of user identification, profiles, authorizations, and password files. Additionally, the National Human Resources Records Manager will oversee and documents how records created regarding this deployment will be retained, scheduled, and disposed of using General Records Schedule 20 (items 1 through 19 and 24). Records schedules are included in Appendix E. Please note that electronic records may not be destroyed unless authorized by a Standard Form 115 that has been approved by the National Archives and Records Administration (NARA).

4.4 Quality Assurance and Reviews

Each State/Center Chief Information Office shall conduct at a minimum a pre-deployment, mid-deployment, and post-deployment review. Reviews are to be documented within the deployment schedule. The e-authentication project manager or his representative shall attend the pre-deployment meeting to help clarify expectations. The reviews will be a self-assessment, but each State/Center may be subject to an independent review of their processes.

a) The objective of the reviews is to document the requirements needed to successfully deploy logical access within the jurisdiction and to ensure requirements are being met.

b) The first review shall take place at least one week prior to commencing work and subsequent reviews shall be set up and scheduled from that start date.

c) Each State/Center CIO shall assemble the team responsible for doing the work. The CIO shall designate a team lead who will be responsible for managing the products, such as deployment schedule, project plan, training plan, project schedules, etc. Roles and Responsibilities will be assigned and overall objectives will be discussed. All records of decisions and meeting minutes will be documented and retained in accordance with GRS schedule.

d) The table below shows the positions and names of the national level team members.

Name	*Job Title*
David Cavellier, BLM, NIRMC	*IT Security Manager*
Dan Boss, BLM, Id	*System Administrator*
Ken Wilbert, BLM, NIRMC	*Network Administrator*
Kathryn Rader, BLM, NIRMC	*Help Desk Administrator*
Tom Newell, BLM, NIRMC	*Configuration Manager*
Robert Martinez, BLM, NHRC	*Records Manager*
Andrew Goldsmith, BLM, WO	*End-User*
Dave Pearson, BLM, NIRMC	*Facilities Manager*
Linda Johnson, BLM, NTC	*Training Coordinator*

e) The documentation required for review is the Project Plan, State Deployment Plan, User Guide, Pre-Deployment and Post-Deployment Documents.

f) The team lead shall create a log to record the outcomes of all requirements/work tasks. If task is achieved, it will be closed out. If the task is not achieved, then its resolution shall be recorded and tracked. The log shall be reviewed by the CIO at least bi-monthly.

g) The CIO shall outline thresholds for decision-makers describing types of approvals required at each milestone.

4.5 Training

Training for State IT Security Managers has been provided at the National Training Center. A second training session has been conducted at Portland Oregon for certificate issuers.

5 DEPLOYMENT SCHEDULE

This section contains the high level breakdown of the project schedule. The detailed project and deployment schedule is included in the Integrated Project Schedule. The Integrated Project Schedule is maintained by the Project Manager and is updated as changes occur.

Responsible Person	Description of Task	Target Date
Project Manager	Kick-off Meetings with States/Centers	July 2004
Point of Contact	Validate Inventories	June 2004
Point of Contact	Distribute Remaining Inventory Stores	June 2004
NTC & Project Office	Conduct Training	March & May 2004
CIO	Sign IATO	June 2004
IT Security	Begin Issuance of Identity Certifications	July 2004
IT Security	Complete Issuance of Identity Certifications	September 2004
State/Center CIOs	Submit Approved Deployment Plans	July 2004
NIRMC CM	Distribute MSI file for ActivCard Gold	June 2004
State/Center CIOs	Push ActiveCard Gold to Desktop	July 2004
Project Manager	Close-out Meetings with States/Centers	December 2004

6 RESOURCES

Employees are required to use Microsoft Excel spreadsheets to track inventories and budget related issues. All plans shall be done in Microsoft Word and project schedules in Microsoft Project or Primavera. A format for inventories is included in Appendix A. The resources identified within Section 1, and Section 4 are the minimal resources required to complete the work. Additional resources shall be identified and documented in the plan as appropriate.

7 PLAN MAINTENANCE

This section describes how the Plan will be kept current.

The Project Manager is responsible for keeping this plan current. The Plan will be updated as significant changes to the system architecture or scope occur.

7.1 List of Acronyms and Abbreviations

BLM – Bureau of Land Management
CIO – Chief Information Officer
DOI – Department of Interior
GRS – General Records Schedule
NTC – National Training Center
OCIO – Office of the Chief Information Officer
PKI – Public Key Infrastructure

7.2 Volume Glossary

Deployment – The distribution of equipment, software and material systematically or strategically.

Logical Access – The use of a PKI digital certificate contained on a smart card, in combination with a personal identification number, to log on to a computer, computer system or computer network.

7.3 Additional Sections (4.3 thru 4.X)

There are no additional sections.

8 ILLUSTRATIONS, TABLES, AND FIGURES

There are no additional illustrations, tables or figures.

APPENDICES

This section may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each Appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendices may be bound as separate documents for ease in handling. Appendices shall be lettered alphabetically (A, B, etc.)

APPENDIX A: INVENTORY

Logical Access Inventory

ITEM	Number Required	Number Acquired	Number Distributed/Installed	Number on Order
Hardware				
Readers - Keyboards	4,250 *	4,500	2,330	0
Readers - USB standalone	2,250	2,250	225	0
Readers – PCMCIA card	2,250	2,250	225	0
Total Readers :	**11,000**	**9,000**	**2,780**	**0**
Smart Cards	15,000	15,000	12,000	0
Other hardware (See items and quantity in section 4.2.1 above)				
Software				
Digital Certificates	9,000	9,000	2,000	0
ActiveCard Gold	Enterprise License	10,000 (each license per user, not per seat)	NIRMC pushed to States/Centers	0
Other Software (See items and quantity in section 4.2.1 above)				

* 2,000 keyboard readers to be acquired by States/Centers through FY03 & 04 Consolidated pc procurement

APPENDIX B: KEYBOARD READER DISTRIBUTION

State	Estimated Number of employees	**Total Number of Keyboards Provided in 1st Distribution**	Percentage of Keyboards Provided in 1st Distribution	Percentage of Keyboards to provide to each State in the Second Distribution	**Number of additional keyboards WO *WILL* provide**	**Total number of keyboards to be provided to each state**	Total Percentage of estimated need provided to each state
AK	1015	0	0	21%	213	**213**	21%
AZ	649	110	17%	4%	26	**136**	21%
CA	1072	0	0	21%	225	**225**	21%
CO	723	0	0	21%	152	**152**	21%
ES	250	110	44%	0	0	**110**	44%
FA	449	0	0	21%	94	**94**	21%
ID	872	720	83%	0	0	**720**	83%
MT	692	0	0	21%	145	**145**	21%
NIFC	323	100	31%	0	0	**100**	31%
NIRMC	569	300	53%	0	0	**300**	53%
NM	933	0	0	21%	196	**196**	21%
NTC	92	90	98%	0	0	**90**	98%
NV	1099	0	0	21%	231	**231**	21%
OR	2475	400	16%	5%	120	**520**	21%
UT	866	0	0	21%	182	**182**	21%
WO	527	400	76%	0	0	**400**	76%
WY	873	100	11%	10%	83	**183**	21%
TOTAL	**13479**	**2330**	**17%**	**13%**	**1667**	**3997**	**30%**
REMAINING NUMBER OF KEYBOARDS IN STOCK: 503							

APPENDIX C: PCMCIA READER DISTRIBUTION

State	Estimated Number of employees	Percentage of Need Provided to State	Calculated Number of PCMCIA Cards to Distribute	Number of PCMCIA Cards to Distribute
AK	1015	16%	162.4	162
AZ	649	16%	103.84	103
CA	1072	16%	171.52	**171**
CO	723	16%	115.68	**115**
ES	250	16%	40	**40**
FA	449	16%	71.84	**71**
ID	872	16%	139.52	**139**
MT	692	16%	110.72	**110**
NIFC	323	16%	51.68	**51**
NIRMC	569	16%	91.04	**91**
NM	933	16%	149.28	**149**
NTC	92	16%	14.72	**14**
NV	1099	16%	175.84	**175**
OR	2475	16%	396	**396**
UT	866	16%	138.56	**138**
WO	527	16%	84.32	**84**
WY	873	16%	139.68	**139**
BLM TOTAL	**13479**		**2156.64**	**2148**
REMAINING NUMBER OF PCMCIA IN STOCK: 102				

APPENDIX D: USB STAND ALONE READER DISTRIBUTION

State	Estimated Number of employees	Percentage of Need Provided to State	Calculated Number of USB Standalone to Distribute	Number of USB Standalone Readers to Distribute
AK	1015	16%	162.4	**162**
AZ	649	16%	103.84	**103**
CA	1072	16%	171.52	**171**
CO	723	16%	115.68	**115**
ES	250	16%	40	**40**
FA	449	16%	71.84	**71**
ID	872	16%	139.52	**139**
MT	692	16%	110.72	**110**
NIFC	323	16%	51.68	**51**
NIRMC	569	16%	91.04	**91**
NM	933	16%	149.28	**149**
NTC	92	16%	14.72	**14**
NV	1099	16%	175.84	**175**
OR	2475	16%	396	**396**
UT	866	16%	138.56	**138**
WO	527	16%	84.32	**84**
WY	873	16%	139.68	**139**
BLMTOTAL	13479	16%	2156.64	**2148**
REMAINING NUMBER OF USB STANDALONE READERS IN STOCK: 102				

APPENDIX E: GENERAL RECORDS SCHEDULE 24

Information Technology Operations and Management Records

This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Information Technology Management Reform Act of 1996 (now the Clinger-Cohen Act), "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

This GRS does not cover all records relating to information technology operations and management. Offices with responsibility for IT operations also maintain administrative records covered by other GRS and records not in the GRS that must be scheduled by the agency. In addition, this GRS does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.

The disposition instructions apply to records regardless of physical form or characteristics. Records may be maintained on paper, in microform, or electronically. Dispositions apply, however, only to records that are maintained as described in each item or sub-item. If documents are part of a larger case file or record keeping system that contains records not covered in this GRS, agencies must separately schedule that file or system by submitting an SF 115 to NARA. If records covered by more than one item in this schedule are maintained together in one file or record keeping system, agencies must retain the records for the longest retention period authorized for those items.

Note that GRS 20, Electronic Records, remains in effect. GRS 20 covers certain temporary files associated with data base management. This new schedule supplements GRS 20 by providing disposal authority for temporary records relating to overall IT management, as opposed to the operation and use of specific systems. NARA is reviewing alternatives to GRS 20 and will develop revised requirements as it explores new approaches to managing electronic records.

1. Oversight and Compliance Files.

   Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

   a. Performance measurements and benchmarks.

      Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

b. All other oversight and compliance records, including certification and accreditation of equipment, quality assurance reviews and reports, reports on implementation of plans, compliance reviews, and data measuring or estimating impact and compliance.

Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

[**Note**: See item 3b for performance files relating to systems.]

2. IT Facility, Site Management, and Equipment Support Services Records.

Records maintained by offices responsible for the control and operation of buildings and rooms where IT equipment, systems, and storage media are located, including files identifying IT facilities and sites, and files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.

3. IT Asset and Configuration Management Files.

a. Inventories of IT assets, network circuits, and building or circuitry diagrams, including equipment control systems such as databases of barcodes affixed to IT physical assets.

Destroy/delete 1 year after completion of the next inventory.

b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes, but is not limited to:

(1) Data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release or version management.

Destroy/delete 1 year after termination of system.

(2) Records of routine IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective (enhancement) maintenance

actions, including requests for service, work orders, service histories, and related records.

Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner.

[**Note**: If any maintenance activities have a major impact on a system or lead to a significant change, those records should be maintained as part of the item 3b(1).]

4. System Backups and Tape Library Records.

a. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

(1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

(2) Delete/destroy full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

[**Note**: See GRS 20, item 8, for backups of master files and databases.]

b. Tape library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs.

Destroy/delete when superseded or obsolete.

5. Files Related to Maintaining the Security of Systems and Data.

a. System Security Plans and Disaster Recovery Plans.

Destroy/delete 1 year after system is superseded.

b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Destroy/delete 1 year after system is superseded.

6. User Identification, Profiles, Authorizations, and Password Files, EXCLUDING records relating to electronic signatures.

   a. Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.

      Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

   b. Routine systems, i.e., those not covered by item 6a.

      See GRS 20, item 1c.

7. Computer Security Incident Handling, Reporting and Follow-up Records.

   Destroy/delete 3 years after all necessary follow-up actions have been completed.

8. IT Operations Records.

   a. Workload schedules, run reports, and schedules of maintenance and support activities.

   Destroy/delete when 1 year old.

   b. Problem reports and related decision documents relating to the software infrastructure of the network or system.

   Destroy/delete 1 year after problem is resolved.

   c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports.

   Destroy/delete when 3 years old.

9. Financing of IT Resources and Services.

[**Note**: Copies of records needed to support contracts should be in procurement files, which are scheduled under GRS 3.]

a. Agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, and non-disclosure agreements.

Destroy/delete 3 years after agreement is superseded or terminated.

b. Files related to managing third-party services, including records that document control measures for reviewing and monitoring contracts and procedures for determining their effectiveness and compliance.

Destroy/delete 3 years after control measures or procedures are superseded or terminated.

c. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency's cost accounting system, which are covered in GRS 8, items 6 and 7.

Destroy/delete records with no outstanding payment issues when 3 years old.

10. IT Customer Service Files.

a. Records related to providing help desk information to customers, including pamphlets, responses to "Frequently Asked Questions,"' and other documents prepared in advance to assist customers.

Destroy/delete 1 year after record is superseded or obsolete.

b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting.

Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

11. IT Infrastructure Design and Implementation Files.

Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting (1) requirements for and implementation of functions such as maintaining network servers, desktop computers, and other hardware, installing and upgrading network operating systems and shared applications, and providing data telecommunications; (2) infrastructure development and maintenance such as acceptance/accreditation of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with implementation, modification, and troubleshooting; (3) models, diagrams, schematics, and technical documentation; and (4) quality assurance reviews and test plans, data, and results.

a. Records for projects that are not implemented.

Destroy/delete 1 year after final decision is made.

b. Records for projects that are implemented.

Destroy/delete 5 years after project is terminated.

c. Installation and testing records.

Destroy/delete 3 years after final decision on acceptance is made.

[**Note**: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]

12. Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this GRS 24 schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
1. Oversight and Compliance Files Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities. a. Performance measurements and benchmarks. Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer. b. All other oversight and compliance records, including certification and accreditation of equipment, quality assurance reviews and reports, reports on implementation of plans, compliance reviews, and data measuring or estimating impact and compliance. Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer. [Note: See item 3b for performance files relating to systems.]	*Statistical performance data for systems and networks; System availability reports; Sample performance indicators* *Target IT architecture reports; Systems development lifecycle handbooks; Network assessments; Contractor evaluation reports; Market analyses; Performance surveys; Cost-benefit analyses; Histograms; Corrective action reports*
2. IT Facility, Site Management, and Equipment Support Services Records. Records maintained by offices responsible for the control and operation of buildings and rooms where IT equipment, systems, and storage media are located, including files identifying IT facilities and sites, and files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence. Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.	*Listings of facilities; Inspection reports*
3. IT Asset and Configuration Management Files. a. Inventories of IT assets, network circuits, and building or circuitry diagrams, including equipment control systems such as databases of barcodes affixed to IT physical assets. Destroy/delete 1 year after completion of the next inventory. b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational	*Maintenance IT assets:* *Inventories of assets, Equipment control systems; Databases of barcodes; Bar code reports; Maintenance service histories;*

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
networks and systems. Includes, but is not limited to: (1) Data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release or version management. Destroy/delete 1 year after termination of system. (2) Records of routine IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective enhancement) maintenance actions, including requests for service, work orders, service histories, and related records. Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner. NOTE: If any maintenance activities have a major impact on a system or lead to a significant change, those records should be maintained as part of the item 3b(1).	*Asset management guides, Service; Requisitions for equipment maintenance; Change orders; Purchase orders for maintenance; Property transfer control systems; Flow reconfiguration requests; Standardization requests and justifications.*
4. System Backups and Tape Library Records. a. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data. (1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later. (2) Delete/destroy full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later. [Note: See GRS 20, item 8, for backups of master files and databases.] b. Tape library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs. Destroy/delete when superseded or obsolete.	*Backup tapes; Backups of system software* *Location vault lists; Offsite storage facilities; Bin location*
5. Files Related to Maintaining the Security of Systems and Data. a. System Security Plans and Disaster Recovery Plans. Destroy/delete 1 year after system is superseded. b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data. Destroy/delete 1 year after system is superseded.	*Computer technical manuals; Continuity of Operations plans; Disaster exercise evaluations; Disaster exercises; Disaster recovery plans; Risk surveys; Security plans for IT*

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
	infrastructure; Vulnerability assessments by IG; Vulnerability assessments/studies *Risk management analyses; Security directives; Security policy analysis; Virus handbooks; Vulnerability analyses*
6. User Identification, Profiles, Authorizations, and Password Files EXCLUDING records relating to electronic signatures. a. Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records. Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later. b. Routine systems, i.e., those not covered by item 6a. See GRS 20, item 1c.	*User identification; User profiles; User passwords Profiles; User authorizations*
7. Computer Security Incident Handling, Reporting and Follow-up Records Destroy/delete 3 years after all necessary follow-up actions have been completed.	*Reports and documentation of Web site defacement; Hacks; Break-in records; Improper usage by staff; Misuse of system; Security breaches; Security break-ins; Security failures; Unauthorized intrusions; Virus threats*
8. IT Operations Records a. Workload schedules, run reports, and schedules of maintenance and support activities. Destroy/delete when 1 year old. b. Problem reports and related decision documents relating to the software infrastructure of the network or system. Destroy/delete 1 year after problem is resolved.	*Cycle time reports; Maintenance schedules; Run reports; Workload schedules* *Software problem reports*

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports. Destroy/delete when 3 years old.	*Benchmark measures; Operation reports; Performance monitoring*
9. Financing of IT Resources and Services [Note: Copies of records needed to support contracts should be in procurement files, which are scheduled under GRS 3.] a. Agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, and non-disclosure agreements. Destroy/delete 3 years after agreement is superseded or terminated. b. Files related to managing third-party services, including records that document control measures for reviewing and monitoring contracts and procedures for determining their effectiveness and compliance. Destroy/delete 3 years after control measures or procedures are superseded or terminated. c. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency's cost accounting system, which are covered in GRS 8, items 6 and 7. Destroy/delete records with no outstanding payment issues when 3 years old.	*Acquisition; Contract award fees; Financial mgmt; Financial records; Payment for software and services; Performance agreements; Service level agreements; Service support levels; Third party agreements*
10. IT Customer Service Files a. Records related to providing help desk information to customers, including pamphlets, responses to ``Frequently Asked Questions," and other documents prepared in advance to assist customers. Destroy/delete 1 year after record is superseded or obsolete. b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting. Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.	*Customer queries; Customer service; End-user inquiries; Feedback records; FAQs; Help Desk logs; Pamphlets; Requests for assistance; Trend analysis; Trouble reports; User guides*
11. IT Infrastructure Design and Implementation Files Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting (1) requirements for and implementation of functions such as maintaining network servers, desktop computers, and other hardware, installing and upgrading network operating systems and shared applications, and providing data telecommunications; (2) infrastructure development and maintenance such as acceptance/ accreditation of infrastructure components, analysis of component options, feasibility, costs and benefits, and work associated with	*Acquisition; Implementation of new systems; Installation and testing; Installation reviews; New enterprise projects; Quality assurance plans;*

GRS 24 Schedule Items	Examples of Types of Records
implementation, modification, and troubleshooting; (3) models, diagrams, schematics, and technical documentation; and (4) quality assurance reviews and test plans, data, and results. a. Records for projects that are not implemented. Destroy/delete 1 year after final decision is made. b. Records for projects that are implemented. Destroy/delete 5 years after project is terminated. c. Installation and testing records. Destroy/delete 3 years after final decision on acceptance is made. [Note: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]	*Requirements specifications; Technology refresh plans; Test plans*
12. Electronic Mail and Word Processing System Copies. Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this GRS 24 schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination. a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy. Destroy/delete within 180 days after the recordkeeping copy has been produced.	*Copies of records in this GRS 24 created using electronic mail and word processing*

GRS 24 Implementation Aid

GRS 24 Schedule Items	Examples of Types of Records
b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. Destroy/delete when dissemination, revision, or updating is completed.	