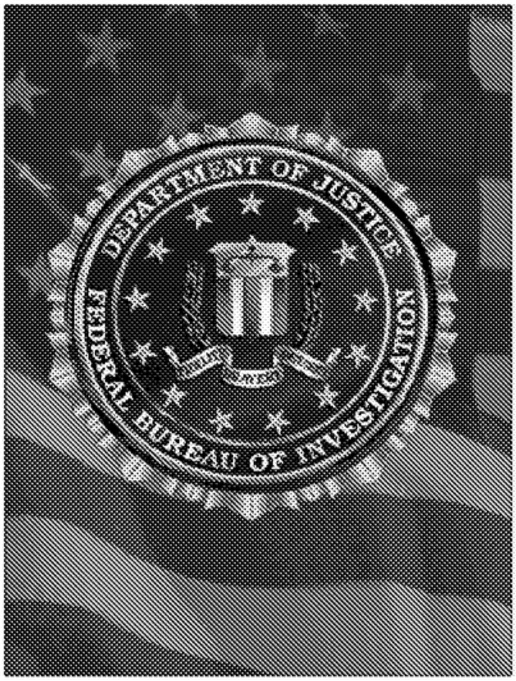
Electronic Recordkeeping Certification

Policy Guide



Federal Bureau of Investigation

Records Management Division

0800PG

August 14, 2015

General Information

Questions or comments pertaining to this policy guide can be directed to:

Federal Bureau of Investigation Headquarters, Records Management Division

Division point of contact: Unit Chief, Records Management Application Unit, [redacted]

b6
b7C

Supersession Information

This document supersedes the *FBI Electronic Recordkeeping Certification Manual,* dated April 30, 2004; 66F-HQ-A1358157-POLI serial 157; 319O-HQ-A1487617 serial 17, and Policy Directive 0249D, *Metadata Tagging of Electronically Stored Information in FBI Systems*.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit or individual(s) listed in the contact section of this policy guide.

Table of Contents

List of Appendices

List of Figures

1. Introduction

The Federal Bureau of Investigation (FBI) is required by statute to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[1] This practice of maintaining "adequate and proper documentation"[2] is essential to efficient and economical agency operations because it ensures that information is documented in official files, including electronic recordkeeping (ERK) systems, where it will be accessible to all authorized staff.

As the FBI continues to advance from paper-based records to electronic records and electronic information management systems, the emphasis must shift from managing physical documents to designing systems that integrate processes and procedures for the creation and management of record content and associated metadata. These systems containing records must comply with the policies and procedures governing the management of federal records.

The FBI adheres to the electronic recordkeeping certification (ERKC) process to ensure that electronic information systems comply with federal records requirements. The Records Management Application Unit (RMAU) of the Records Management Division (RMD) leads the certification process in collaboration with system owners. Development of new information or knowledge management (KM) systems may continue without certification; however, it is incumbent on the project manager (PM) and system owner for any information or KM system in development to ensure coordination with RMAU and obtain certification.

Implementation of the ERKC process ensures that the systems the FBI develops and maintains comply with statutory and agency ERK requirements. The ERKC process incorporates ERK requirements into the system development life cycle (SDLC) so that all system development activities can appropriately consider ERK criteria from the earliest stages of acquisition and design.

The ERKC process evaluates system compliance with records management (RM) criteria. The process is designed to guide system owners and developers in assessing and incorporating RM criteria into system requirements specifications and to ensure fulfillment through the review of documented test results. The ERKC process consists of identifying systems that contain records; helping system owners, PMs, and developers understand ERK criteria; ensuring that system requirements specifications satisfy ERK criteria; and validating ERK functionality through the review of system test results. The ERKC process is designed to leverage the outputs from existing information technology (IT) systems management processes to minimize redundant data capture and reduce the burden on systems development and management activities.

1.1. Purpose

The goal of the ERKC process is to ensure that electronic information systems comply with statutory and agency ERK criteria, including requirements for the proper creation, maintenance, use, and disposition of FBI records. These requirements should be incorporated into the design and deployment of new electronic information and KM systems (hereafter collectively referred

[1] The Federal Records Act, 44 U.S.C. Section (§) 3101 (1950)

[2] This phrase was originally used in the Federal Records Act of 1950, which established records management as a basic responsibility of all federal agencies.

to as "electronic information systems") and ensure that all existing FBI systems are also in compliance.

The *Electronic Recordkeeping Certification Policy Guide* accomplishes the following objectives:

- It defines the authorities, roles, responsibilities, processes, and documentation requirements that govern the certification of FBI-owned and FBI-sponsored IT systems.
- It serves as a guide for system developers, system owners, PMs, and certification team members to the activities required for FBI-owned and FBI-sponsored systems to obtain ERKC.

1.2. Intended Audience

This PG is intended for IT system owners, PMs, and developers, as well as the RMAU certification team.

2. Roles and Responsibilities

This section summarizes the primary roles and responsibilities of the two principal participants in the ERKC process. Subsection 2.1. describes the responsibilities of the system owner. Subsection 2.2. describes the responsibilities of RMAU.

2.1. System Owners

The system owner's role is to ensure that the FBI electronic information systems for which he or she is responsible meet the FBI ERK criteria. In operating the systems and participating in ERKC activities, system owners must:

- Notify RMAU of all planned new electronic information systems and existing legacy electronic information systems by completing the Electronic Systems Questionnaire (ESQ) during early system planning and development.
- Meet with RMAU, when requested, to help determine whether electronic information systems contain records.
- Develop and incorporate the appropriate ERK criteria into the electronic information system requirements specifications and integration/acceptance test plans (in consultation with RMAU, if so desired).
- Provide standard electronic information system documentation (e.g., system security plans, user guides, system administration manuals, system design documents), as requested by RMAU, to support the ERKC process.
- Comply with the terms and conditions of the appropriate certification (i.e., approval to operate [ATO], interim approval to operate [IATO], and no approval to operate [NATO]) for each electronic information system.
- Notify RMAU of any planned changes to any electronic information system operating under an ERK ATO that affect data management of the system, which in turn might adversely affect the ERKC.
- Determine the feasibility of successfully executing risk mitigation plans (RMPs), and notify RMAU. Feasibility is determined using factors that include, but are not limited to, time to execute, cost, and technical constraints.
- Cooperate with RMAU for system review and recertification activities by coordinating a Privacy Impact Assessment (PIA) from the Office of the General Counsel (OGC) and a Security Assessment and Authorization (SAA) from the Security Division (SecD) for each electronic information system granted an ERK ATO.
- Notify RMAU of the changes being made to address risks identified during the ERKC process that result in an ERK IATO or NATO determination.

2.2. Records Management Application Unit

The principal role of RMAU is to determine whether FBI systems contain records. If a system is determined to contain records, RMAU certifies whether the system meets FBI criteria for an ERK system. In performing ERKC activities, RMAU must:

- Determine, in consultation with system owners, whether an electronic information system contains records (for legacy electronic information systems) or will contain records once implemented (for new electronic information systems).
- Determine, for data created and maintained on the electronic information system, records disposition guidelines that will meet the operational needs of the program office, the statutory needs for the FBI, and the historical documentation needs of the National Archives and Records Administration (NARA).
- Provide advice and guidance to system owners when they are selecting their preferred approaches to meeting ERK criteria.
- Provide assistance on the development of the ERKC portions of test plans.
- Review and evaluate electronic information system documentation, from an ERKC perspective, and report the results of the ERKC evaluation.
- Determine whether the validation of ERK functions by demonstration is required, and notify system owners of the requirement.
- Perform risk analyses, as needed, for electronic information systems to determine whether the risks posed by electronic information systems that do not meet all ERK criteria are acceptable.
- Prepare RMPs for electronic information systems that do not meet all ERK criteria.
- Determine the appropriate ERK certification (i.e., ATO, IATO, or NATO) for each electronic information system.
- Review electronic information systems operating under ATO and IATO no less than every three years, and determine whether to grant recertification (i.e., a new ATO), issue an IATO, or issue a NATO for these electronic information systems.

3. Policies

All FBI-owned and FBI-operated electronic information systems used to process FBI information, regardless of where they operate, must undergo the ERKC process in accordance with the procedures described in this PG.

4. Procedures and Processes

This section describes the ERKC process for both new and legacy systems. While ERK criteria are the same for both new and legacy systems, the processes for obtaining certification are different. Subsection 4.1. describes the ERKC process for new systems; subsection 4.2. describes the ERKC process for legacy systems. Subsection 4.3. discusses the risk management analysis conducted for both new and legacy systems.

The ERKC process described in this PG is the FBI's official process for evaluating the technical and nontechnical electronic RM features of FBI information systems and for determining whether those features satisfy the ERK compliance criteria. RMAU must determine the potential implications of noncompliance with ERK criteria. The "Comment" column in the ERK Compliance Evaluation Worksheet may be used to record the implications. The certification determination may take one of the following forms:

- ATO: an approval to operate a system because the system meets all recordkeeping criteria (ATOs must be recertified every three years).
- IATO: a temporary approval to operate a system for a defined period of time and under certain defined conditions.
- NATO: a denial of approval to operate a system because it fails to meet recordkeeping criteria.

Systems that contain, or will contain, records in non-textual formats, such as digital photographs, digital audio, and geospatial data, are also evaluated during the records assessment and ERKC processes. This evaluation is required to ensure readability of the data for the entire records retention life cycle. Software obsolescence, proprietary format issues, and other factors can hamper readability as electronic information systems are upgraded or replaced. When establishing system requirements, system owners should contact RMAU to determine the additional data retention challenges for these types of formats. Owners of legacy systems containing data in these formats should work with RMAU to determine any risks associated with the formats so that risk mitigation can be implemented, thereby avoiding loss of data due to technological obsolescence and ensuring readability throughout the required records life cycle.

4.1. ERKC Process for New Systems

The ERKC process for new systems requires system owners and RMAU to undertake activities in all four phases of the ERKC life cycle: namely, the definition phase, verification phase, validation phase, and post-certification phase. The sections below describe these activities and provide a simplified checklist approach to outline who performs needed functions and tasks and who must produce certain written products to support the certification process.

4.1.1. Definition Phase

The definition phase begins when RMAU becomes aware of a potential new system. This phase may be triggered by the flow of certain documentation (e.g., business plans in the form of Exhibit 300s or Exhibit 53s, system security plans, or application architectures) through RMD or IT life cycle management working groups and boards. Once aware of the system, RMAU must work with the system owner to determine whether the system will contain records. If not, the process stops and RMAU must make entries into the RMAU tracking and control system and the

Bureau Information Technology Knowledge Repository (BIKR) to reflect that the system does not contain records. The program office and the IT portfolio manager and/or PM for the system must be notified of this determination by RMAU through an electronic communication (EC), which must contain a basic description of the system, indicate that the system does not contain records, and include the basis for the determination. The notification EC is maintained by RMD in the 319U-HQ-A1487670-RMD file.

A classification 242 case file must be established for uploading documentation related to the management of each system (refer to Section 6 of this PG for more information). RMAU will establish the 242 case file in coordination with either the system owner or program manager. If the system will contain records, RMAU and the system owner must create a records disposition schedule. A records disposition schedule provides specific and mandatory instruction for the management of records created, maintained, and used by systems during the conduct of FBI operations and specifies the overall retention of the records once the operational needs have been met. A records disposition schedule may already exist, or one may need to be developed. Records disposition schedules, once drafted to meet the business needs of the program office, must be coordinated with RMAU and approved by NARA.

If RMAU determines that the records being maintained by a system will require retention in the system for ten years or less, RMAU must cite appropriate records disposition guidance formally with a notification EC, and the system will not require ERKC.

Figure 1 illustrates the steps in the definition phase, including who is responsible for each action and what products (if any) must be produced at each step by each party (i.e., RMAU or system owner).

New System ERKC Definition Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
1 Review available system documentation (e.g., Exhibit 300s, Exhibit 53s, system security plans, application architectures) to identify new systems.	Entry in RMAU ERKC tracking system.		
2 Meet with the system owner to determine whether system will contain records.	Description of the system for inclusion within the RMAU tracking system and an indication of whether system contains records	2 Meet with RMAU to determine whether system will contain records.	
If "YES," proceed to Step 3 and Step 4.		If "YES," proceed to Step 3.	

New System ERKC Definition Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
If "NO," issue a notification EC.	Notification EC	If "NO," stop.	
		3 Manage system development materials in accordance with classification 242 guidelines, and establish use of BIKR to track. Establish a classification 242 case file under the guidelines of Section 6 of this PG.	242 case file in Sentinel
4 Assist system owner in establishing ERK approach. Determine if records will be managed under an existing records schedule, or if a new records schedule should be developed.	Records disposition guidance or new draft records schedule, as appropriate Update to RMAU ERKC tracking system	4 Meet with RMAU to discuss ERK requirements and determine if records disposition requirements can be addressed within existing system functions.	

Figure 1. ERKC Definition Phase – New System

4.1.2. Verification Phase

The verification phase follows the definition phase. Its purpose is to ensure the inclusion of ERK criteria in system requirements specifications and test plans. This will enable the system to meet ERK criteria when it undergoes subsequent integration and acceptance testing. Figure 2 illustrates the steps and products associated with this phase. The ERK assessment criteria, sample tests, and expected results are provided in Appendix E.

New System ERKC Verification Phase: Activities and Products			
RMAU		System Owner	
Activity	**Product**	**Activity**	**Product**
5 Assist system owner in understanding ERK criteria (as requested by system owner).	Copy of records schedule (or proposed records schedule)	5 Understand ERK criteria sufficiently to develop system requirements.	
6 Assist system owner in incorporating necessary ERK criteria into system requirements documentation (as requested by system owner).	Comments and recommendations on system requirements documentation	6 Develop system requirements documentation, incorporating necessary ERK criteria.	System requirements documentation addressing ERK criteria.
7 Assist system owner in incorporating necessary ERK criteria into test plan (as requested by system owner).	Comments and recommendations on test plan	7 Develop the system integration and/or acceptance test plans, incorporating necessary ERK criteria.	Test plan

Figure 2. ERKC Verification Phase – New System

4.1.3. Validation Phase

The validation phase begins following the development of the test plan. During this phase, the system owner must conduct integration/acceptance testing in accordance with the test plan. RMAU must review the results of testing and other system documentation (such as the PIA from OGC and the system security documentation from SecD) to validate compliance with ERK criteria. RMAU must then produce a system certification report and issue an ERK ATO if the system meets all ERK criteria. If areas of noncompliance are identified, an ERK IATO must be issued, and RMAU must prepare an RMP. Figure 3 illustrates the steps and products associated with this phase.

RMAU must review ERK ATO determinations every three years, or prior to major system changes. A system entering, or currently in, the product development process as of (or following) the effective date of this PG are required to achieve an ERK ATO upon becoming fully operational. If the system fails to achieve an ERK ATO and an ERK IATO is issued, the system owners and developers must devise a plan to achieve ERK ATO by the next review, in accordance with the three-year review cycle. The plan must be submitted to RMAU within 120 days of ERK IATO notification.

ERK NATO determinations will preclude the use of the system to conduct FBI business. If a system receives an ERK NATO, RMD must notify the Director of the FBI, the Information Technology Customer Relationship and Management Division (ITCRMD), OGC, SecD, and the system owner and/or PM. The system must be taken offline, or identified risks must be mitigated within 30 days.

New System ERKC Validation Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
8 Support integration/ acceptance testing (as requested by the system owner).	Comments and recommendations on conduct of integration/acceptance testing	8 Conduct the integration/ acceptance testing and document the test results. Provide a copy of the results to RMAU.	Test results
9 Review the test results and system documentation to determine whether all ERK criteria have been met. If "YES," certify the system by granting ATO. Proceed to Step 12 (subsection 4.1.4., "Post-Certification Phase"). If "NO," proceed to Step 10.	System certification report and ATO	9 If "YES," proceed to operate the system; go to Step 12 (subsection 4.1.4., "Post-Certification Phase"). If "NO," proceed to Step 10.	
10 Determine whether existing risks are acceptable. If "YES," issue IATO (not to exceed one year). Proceed to Step 11. If "NO," work with the program office to create a mitigation plan that meets both program office and RMAU requirements.	System certification report, RMP, and IATO	10 If "YES," operate system under the terms of the IATO. Provide RMAU with an implementation plan within 90 days. If "NO," work with RMAU to revise the mitigation plan and create an implementation plan that meets both program office and RMAU needs.	Written acknowledgement of the terms of the IATO and implementation plan Revised mitigation plan and implementation plan

New System ERKC Validation Phase: Activities and Products			
RMAU		System Owner	
Activity	**Product**	**Activity**	**Product**
11 Examine the implementation plan and determine its feasibility.		11 Examine the implementation plan.	Periodic reports of implementation plan progress.
If the plan is feasible (i.e., “YES”), proceed to the next step.		If the plan is feasible (i.e., “YES”), proceed to the next step.	Revised implementation plan.
If the plan is not feasible (i.e., “NO”) work with program office to revise the implementation plan to meet both program office and RMAU needs.		If “NO,” work with RMAU to revise the implementation plan to meet both program office and RMAU needs.	

Figure 3. ERKC Validation Phase – New System

4.1.4. Post-Certification Phase

The post-certification phase has two primary objectives. The first is to enable RMAU to determine whether the terms of any ERK IATO should be extended, or whether the ERK IATO should be changed to an ERK ATO or an ERK NATO. The second is to perform routine, periodic (every three years) reviews of the status of systems granted ERK ATOs to ensure that these systems continue to meet all ERK criteria.

As described in this section, RMAU issues an ERK IATO with certain terms and conditions. In addition, an ERK IATO may accommodate the development and implementation of a system put in place to meet emergency operational needs (e.g., during natural disasters). Similarly, an ERK IATO may authorize the operation of a system in a restricted operational environment (e.g., on a separate local area network not connected to the FBI Intranet) to serve as a proof of concept before implementing its fully ERK-compliant (full ERK ATO) counterpart on a broader scale.

Regardless of the terms and conditions associated with the ERK IATO, the intent of the post-certification phase is to examine the operation of the system covered by the IATO and determine the next appropriate step to be taken. In the case of a system developed for emergency operational needs, the appropriate action may be to disallow continued operations (e.g., the emergency is over) and require all of the records created within the system to be transferred to an approved records management application (RMA) or another system that can properly manage the records for their entire life cycle.

With respect to systems granted ERK ATOs, RMAU must review the operation of these systems every three years to ensure continuing compliance with ERK criteria. This three-year review cycle should correspond with the PIA from OGC and use information from the most current SAA from SecD. Maintaining the certification is contingent upon continued adherence to the provisions of ERK criteria.

Once granted an ERK ATO, a system may undergo changes (e.g., new functionality) that could prevent the system from satisfying the ERK criteria. As upgrades or changes to the system are planned, the system owner must provide change requests through the ITB change request process for pre-coordination by RMAU to ensure that these changes do not alter any recordkeeping aspects of the system. In such cases, RMAU may require further modifications to the system in order to accommodate these criteria.

Figure 4 illustrates the steps and products associated with the post certification phase.

New System ERKC Post Certification Phase: Activities and Products			
RMAU		System Owner	
Activity	**Product**	**Activity**	**Product**
12 Monitor ATO and IATO expiration dates.		12 Operate system under the terms and conditions of the ATO or IATO.	Change requests
13 Notify system owner of recertification requirements.	Recertification notice	13 Provide current versions of system documentation.	Requirements specifications, test results of compliance with conditions of IATO, and the implementation plan
14 Review current system documentation and determine whether all ERK criteria have been met. If "YES," certify the system by granting ATO. Proceed to Step 12. If "NO," proceed to Step 15.	System certification report and ATO	14 Support RMAU review of system documentation. If "YES," continue to operate the system. Proceed to Step 12. If "NO," proceed to step 15.	

New System ERKC Post Certification Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
15 Determine whether existing risks are acceptable.	System certification report, RMP, and IATO	15 Examine issued system certification report and RMP and determine the plan's feasibility.	Written acknowledgement of the terms of the IATO and implementation plan
If "YES," issue IATO.	NATO	If the plan is feasible (i.e., "YES"), provide RMAU with an implementation plan.	Revised implementation plan
		Address risk(s) per implementation plan and provide RMAU with an implementation report.	
If "NO," issue NATO and notify system owner, ITMD, OGC, and Director.		If the plan is not feasible, stop. Discontinue use of the system.	
16 Examine the implementation plan and determine if the system now meets ATO requirements.	System certification report and ATO NATO		
If all risks have been addressed, issue ATO.		16 Operate the system under ATO.	
If risks have not been addressed, issue NATO and notify system owner, ITMD, OGC, and the Director.		If NATO received, stop. Discontinue use of the system.	

Figure 4. ERKC Post-Certification Phase – New System

4.2. ERKC Process for Legacy Systems

The ERKC process for legacy systems requires system owners, PMs, and RMAU to undertake activities in only the last two phases of the ERKC life cycle because legacy systems have already been developed and have undergone integration and acceptance testing. The sections below describe the associated activities and provide a simplified checklist approach that outlines who performs needed functions and tasks and who must produce written products to support the certification process. Because integration and acceptance testing will have already occurred for legacy systems, it may be necessary to develop and conduct a special demonstration of system functions if RMAU is unable to determine, from a review of existing system documentation[3], whether the system complies with ERK criteria.

4.2.1. Validation Phase

The purpose of the validation phase for legacy systems is to determine whether the system satisfies the ERK assessment criteria presented in Appendix D. RMAU should attempt to ascertain this fact by reviewing various documents associated with the system. If sufficient information is not available, RMAU must request that the system owners conduct a specially focused system demonstration.

RMAU must initiate the ERKC process upon learning of a legacy system. Triggers include Exhibit 300s and 53s, revisions to system security plans, and updates to application architecture documents. RMAU must work with the system owner to determine whether the system contains records. If the system does not contain records, no further action by the system owner is required. RMAU must document that the system does not contain records in the RMAU tracking system and issue an EC to the system owner (as discussed in subsection 4.1.1. of this PG).

If the system does contain records, RMAU must determine if a records schedule is already in existence or if one needs to be developed, as discussed in subsection 4.1.1.

If RMAU determines that the records being maintained by a system will only need to be managed by the system for ten years or less, RMAU must cite appropriate records disposition guidance formally with a notification EC and should not require ERKC.

Once records retention requirements are identified for systems containing records that will be maintained more than ten years, RMAU must determine whether the system meets all necessary ERK criteria by reviewing system documentation and the results of the system's integration/acceptance testing. If an appropriate determination cannot be made from these documents, RMAU must request additional documentation (e.g., user guides and system administration manuals); if RMAU still cannot determine whether the system satisfies the needed ERK criteria, RMAU must direct the system owner to conduct a special demonstration of the system functions in question. RMAU must then issue either an ATO or an IATO, providing guidance for the corrective actions needed to achieve ATO. This process will require RMAU to prepare an RMP and the system owner to determine if the plan is feasible. Figure 5 illustrates the steps and products associated with the validation phase for a legacy system.

[3] Existing documentation may include, but is not limited to, test plans, system design documents, requirements specifications, user guides, and system administration manuals.

Legacy System ERKC Validation Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
1 Review available system documentation (e.g., Exhibit 300s, Exhibit 53s, system security plans, application architectures) to identify legacy systems.	Entry in RMAU ERKC tracking system	1 Ensure that system is recorded in BIKR and that system documentation is being managed as part of a 242 classification case. If not, establish a 242 case under the guidelines of Section 6.	BIKR registration number and 242 case file
2 Meet with system owner to determine whether the system contains records.	Description of system for inclusion in the RMAU tracking system and an indication of whether the system contains records	2 Meet with RMAU to determine whether the system contains records.	
If "YES," proceed to Step 3 and determine if records will be managed under an existing records schedule, or if a new records schedule should be developed.	Records disposition guidance or new draft records schedule, as appropriate	If "YES," proceed to Step 3.	
If "NO," issue an EC detailing the decision.		If "NO," stop.	
3 Request requirements specifications, test plans, and test results from system integration/acceptance testing.	Request for system documentation	3 Provide system documentation (as available).	System documentation
4 Review system documentation to determine whether ERK criteria are being met.	System certification report and ATO		
If "YES," issue ATO. If "NO," go to Step 5.			

Legacy System ERKC Validation Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
5 If documentation is insufficient to evaluate compliance, validate ERK criteria through a demonstration. The demonstration should address questions and issues developed to complete the system certification report.	Questions and issues to be addressed by the system demonstration	5 Demonstrate relevant system functionality in support of ERKC evaluation.	System demonstration
6 Review system certification report and determine whether all ERK criteria have been met.	System certification report and ATO		
If "YES," issue an ATO.		6 If "YES," continue to operate the system. Go to Step 11.	
If "NO," proceed to next step.		If "NO," proceed to next step.	
7 Determine whether existing risks are acceptable.	System certification report, RMP, and IATO		Written acknowledgement of the terms of the IATO and implementation plan Revised mitigation plan and implementation plan
If "YES," issue IATO (not to exceed one year). Proceed to Step 11.		7 If "YES," operate system under terms of the IATO. Provide RMAU with an implementation plan within 90 days.	
If "NO," work with the program office to create a mitigation plan that meets both program office and RMAU requirements.		If "NO," work with RMAU to revise the mitigation plan and create an implementation plan that meets both program office and RMAU needs.	

Legacy System ERKC Validation Phase: Activities and Products			
RMAU		System Owner	
Activity	Product	Activity	Product
8 Examine the implementation plan and determine its feasibility.	System certification report, RMP, and IATO	8 Examine the implementation plan.	Periodic reports of implementation plan progress
If the plan is feasible (i.e., "YES"), issue IATO (not to exceed one year).	Revised implementation plan	If the plan is feasible (i.e., "YES"), operate system under terms of the IATO.	Revised implementation plan
If the plan is not feasible (i.e., "NO"), work with program office to revise the implementation plan to meet both program office and RMAU needs.		If the plan is not feasible (i.e., "NO"), work with RMAU to revise the implementation plan to meet both program office and RMAU needs.	

Figure 5. ERKC Validation Phase – Legacy System

4.2.2. Post-Certification Phase

The purpose of the post-certification phase for a legacy system is twofold. First, it enables RMAU to determine whether the terms of any IATO should be extended or whether the IATO should be changed to an ATO or an NATO. Second, it enables RMAU to perform routine, periodic (every three years) reviews of the status of systems granted ATOs to ensure that the systems continue to meet all ERK criteria.

IATOs for legacy systems will have certain terms and conditions associated with them. For example, an IATO may authorize the continued operations of a non-ERK-compliant system for a specified period of time (e.g., 12 months) because the system will be retired or replaced with an ERK-compliant system within this period of time, and the costs of retrofitting the noncompliant system are deemed excessive relative to the risks associated with continued "as is" operation. Similarly, RMAU may issue an IATO for a legacy system because there is a planned upgrade to the system that will make it ERK-compliant within a specified period. Lastly, RMAU may issue an IATO for a legacy system because it was developed and implemented for emergency purposes, and the emergency still exists. The process for post-certification of legacy systems is identical to the post-certification process described for new systems (see subsection 4.1.4. and Figure 4).

4.3. Risk Management

An important aspect of risk management is to determine the potential negative impact with regard to the management of records associated with any criteria for which less-than-complete satisfaction was demonstrated by the PM or owner during an evaluation of system documentation (i.e., criteria for which the compliance value is less than 1). This information must serve as the foundation for any mitigation plan developed to obtain an IATO.

4.3.1. ERKC Report, Risks, and Mitigating Factors

The ERKC evaluator must develop the ERKC report using the completed ERK Compliance Evaluation Worksheet, which is based on the ERK assessment criteria listed in Appendix D, and notes from meetings with the system owner. The report should summarize the results of the system evaluation and focus on descriptions of risks and unique system characteristics that mitigate risks. The report must be organized according to the six criteria classes, as shown in Appendix D, to ensure that related risks are discussed together to provide sufficient context to support a certification decision by RMAU. The final ERKC report consists of this risk analysis supported by the final completed ERK Compliance Evaluation Worksheet.

Each risk identified as a result of the risk analysis process should have a mitigation strategy. Therefore, RMAU must create an RMP when issuing an IATO. A mitigation plan is used to lessen or alleviate the adverse effect of the risk; however, interim countermeasures may also be effective in reducing the system risk level.

Examples of possible mitigation strategies include:

- Using an alternative method of storing records (e.g., printing out and filing records in paper form) until the ability to transfer records to the RMA is built into the system.
- Including the desired feature in the next version of the system upgrade that is funded for the following year.
- Determining that the system is temporary and will outlive its usefulness (or be replaced) within the following year.

The system owner must develop an implementation plan to address identified risks. After RMAU has reviewed and approved the implementation plan, the program office must provide periodic implementation reports documenting when changes are made addressing the identified risks. RMD will review and recertify the system, after changes are implemented, within one year for new systems or three years for legacy systems, as indicated in the EC notifying the system owner of the IATO.

5. Summary of Legal Authorities

- The Federal Records Act of 1950, as amended (Title 44 United States Code [U.S.C.] Chapters 21, 29, 31, and 33)
- The E-Government Act of 2002 (44 U.S.C. Chapter 35)
- NARA Regulations for Federal Agency Records (Title 36 Code of Federal Regulations (CFR) Chapter 12, Subchapter B)
- Office of Management and Budget (OMB) Circular A-130, Section 8a(k)
- Policy Directive (PD) 0457D, *RMD Statement of Authorities and Responsibilities*

6. Recordkeeping Requirements

Classification 242 (Automation Matters) was established to house records related to the design, acquisition, development, implementation, certification, and modification of FBI systems. The creation, maintenance, and retention of system documentation records are necessary for recordkeeping purposes during the full system life cycle. These records provide evidence of the following:

- Procurement
- Development
- Technical requirements
- Implementation
- Maintenance

All legacy and new systems should have a classification 242 main file for the management of system documentation. If not, system owners are required to either establish a case or request RMAU open a case. RMAU has developed a standardized list of system documentation that should be captured in the classification 242 case files, including documentation of the following:

- System design: Includes the concept of operations (CONOPS), project design, and functional requirements documents.
- System development: Includes design, implementation, installation, and testing records, as well as data dictionaries, models, diagrams, schematics, and technical documentation.
- Acquisition and contracting: Includes records related to procurement, the contract bid process, statements of work, requests for proposals, requests for quotes, contracting officer's representative (COR) assignments, and contract deliverables not otherwise documented in contract files.
- System implementation and operations: Includes user guides, operational support and training records.
- SSA under the Federal Information Security Management Act (FISMA): Includes system certification, accreditation, system security plans, and security records.
- ERKC: Includes records related to compliance with ERK requirements.
- Budget and finance: Includes records related to the allotment of funds.
- Meetings: Includes records of review boards and other informal groups. Records include meeting minutes, agendas, briefings, attendees, and correspondence.
- PIAs: Includes records related to the development and approval of PIAs.
- Tracking: Includes status and progress reports, system modifications, and upgrades.

Appendix A: Final Approvals

POLICY TITLE: ***Electronic Recordkeeping Certification Policy Guide***	
Primary Strategic Objective	T7- Deploy technology and science to make our workforce more effective and efficient.
Publish Date	2015-08-14
Effective Date	2015-08-14
Review Date	2018-08-14
EXEMPTIONS	
None	
APPROVALS	
Sponsoring Executive Approval	**Michelle A. Jupina** Assistant Director Records Management Division
Final Approval	**Kevin L. Perkins** Associate Deputy Director

Appendix B: Contact Information

Records Management Division	
Records Automation Section	[redacted]
Records Management Application Unit Unit Chief [redacted]	[redacted]
Records Management Application Unit ERKC Team Lea[redacted]	[redacted]
Records Management Division 170 Marcel Drive Winchester, Virginia 22602	

b6
b7C

Appendix C: Key Words, Definitions, and Acronyms

Key Words

- Electronic recordkeeping
- Electronic recordkeeping certification
- Record
- Information life cycle management
- Information management

Definitions

Approval to operate: a certification to operate a system on a "permanent" basis (in the absence of subsequent modifications to the system), granted by RMAU. Each ATO is good for a period of three years, and recertification must be completed by RMAU for each system operating under an ATO within the three-year window, which begins upon the granting of an ATO for the system.

Category: a records series or a group of records with similar characteristics assigned to a particular records disposition schedule and generally handled as a unit for disposition purposes. In many RMAs, a category is a file folder icon in which records are assigned.

Disposition instructions: actions taken with regard to federal records after the records are no longer required to conduct current agency business. These actions include the following: the transfer of records to agency storage facilities or federal records centers (FRCs); the transfer of records from one federal agency to another; the transfer of permanent records to NARA; and the disposal of temporary records, usually by destruction.

Electronic information system: an information system that contains and provides access to computerized federal records and other information.

Electronic record: any information recorded in a form which only a computer can process and which satisfies the definition of a federal record under the Federal Records Act (see "record" definition below). The term includes both record content and associated metadata that the agency determines is required to meet agency business needs (36 CFR § 1220.18).

Exact match search: a search that returns data which includes the exact search string; also known as an "on-the-nose" search.

File plan: a document that contains the identifying number, title, or description and disposition authority of files held or used in an office.

Global change: an automatic search-and-replace feature. Global changes are performed when one change needs to be made to a number of records. By doing a global change, the new data is keystroked once.

Implementation plan: a plan written by the system owner outlining how identified risks will be corrected to ensure that RM requirements are met.

Implementation report: a report notifying RMAU that the changes outlined in the implementation plan have been completed.

Interim approval to operate: a certification granted by RMAU to operate a system for a temporary period of time and in accordance with specified conditions.

Metadata: preserved contextual information describing the history, tracking, and/or management of an electronic document. Metadata describes information—specifically, its context, content, structure, and management over time. See 36 C.F.R. § 1236.2. This data is needed to build information resources, such as ERK systems, and support records creators and users.

No approval to operate: the denial of approval to operate a system because it fails to meet critical recordkeeping criteria.

Proximity/adjacency searches: searches that return data which include search strings within a certain "distance" of other strings (e.g., when the word "fire" is within 50 characters of "explosion").

Record: according to 44 U.S.C. § 3301:

> [All recorded information], regardless of form or characteristics, made or received by an agency of the United States government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes [and] extra copies of documents preserved only for convenience of reference…are not included.

Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

Records disposition schedule: provides specific and mandatory instructions for the management of records created, maintained, and used by systems during the conduct of FBI operations and specifies the overall retention of the records once the operational needs have been met.

Records Management Application Unit: the designated unit of RMD responsible for reviewing the ERK capabilities of new and legacy systems and determining whether to grant system owners permission to operate the systems from a recordkeeping perspective.

Relevance ranking: a system mechanism that determines the degree to which the retrieved data are relevant to the search.

Risk analysis: the process performed by RMAU to determine the acceptability of the risks posed by a system that does not meet all of the required ERK criteria.

Risk mitigation plan: a plan developed by RMAU that spells out a proposed approach to alleviate the risks posed by a system that does not meet all ERK criteria.

Sealed record: a record that has been redacted and has an identifying border burned into the document so the redacted information may not be reverse-engineered. Sealed documents may not be unsealed.

Stop words: extremely common words that a search engine will not search for in order to save space or speed up searches. Examples include "the," "it," "and," "a," and "or."

System: an information system that contains and provides access to computerized FBI records and other information.

System development life cycle: the design, development, deployment, operation, and maintenance of systems.

System owner: a broad term referring to anyone who manages the acquisition or development of an electronic information system or places an electronic information system into operation. Within the FBI, the CIO and each assistant director (AD) is responsible for the operational management of applications or electronic information systems that directly support his or her business area.

Vital record: a record needed by an agency for continuity of operations before, during, and after emergencies, or a record needed to protect the legal and financial rights of the government and persons affected by government activities.

Wildcard characters: characters that can be used in queries in place of unknown characters and to search for multiple variations of a term. For example, searching "terror*" would retrieve data that include "terror," "terrorist," "terrorism," and similar terms.

Acronyms

AD	assistant director
ASCII	American Standard Code for Information Interchange
ATO	approval to operate
BIIF	Binary Image Interchange Format
BIKR	Bureau Information Technology Knowledge Repository
CFR	Code of Federal Regulations
CONOPS	concept of operations
COR	contracting officer's representative
DMA	document management application
EC	electronic communication
EO	Executive Order
ERK	electronic recordkeeping

ERKC	electronic recordkeeping certification
EXIF	Exchangeable Image File Format
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FRC	federal records center
GIF	Graphics Interchange Format
IATO	interim approval to operate
ID	identification
IT	information technology
ITCRMD	Information Technology Customer Relationship and Management Division
JPEG	Joint Photographic Experts Group
KM	knowledge management
NARA	National Archives and Records Administration
NATO	no approval to operate
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OO	office of origin
PD	policy directive
PDF	Portable Document Format
PG	policy guide
PIA	Privacy Impact Assessment
PM	project manager

PNG	Portable Network Graphics
RM	records management
RMA	records management application
RMAU	Records Management Application Unit
RMD	Records Management Division
RMP	risk mitigation plan
SAA	Security Assessment and Authorization
SDLC	system development life cycle
SecD	Security Division
sRGB	standard red--green--blue
TIFF	Tagged Image Interchange Format
U.S.	United States
URL	uniform resource locator
U.S.	United States
U.S.C.	United States Code

Appendix D: Electronic Recordkeeping Assessment Criteria

This appendix contains the ERK assessment criteria, which have been established by RMD for all FBI recordkeeping information systems. The criteria are the basis on which new and existing systems are evaluated for ERKC. Each criterion is followed by one or more sample functions and expected results that can be used to assist system owners in developing test plans and to support the review of test results by RMAU.

Note: The "user" refers to authorized users only. Different functions are permitted for different groups of users (e.g., administrative functions for records managers, retrieval functions for end users).

<table>
<tr><th colspan="2">1. DECLARE RECORDS</th></tr>
<tr><td colspan="2"><b>Criterion 1.1:</b> The system designates specified information as records, either manually or automatically (once saved, the record cannot be changed).</td></tr>
<tr><td><b>Sample Function</b></td><td><b>Expected Results</b></td></tr>
<tr><td>Import a document into the system. Designate the document as a record.</td><td>Record document is not changed once saved.
Non-record documents in the system are not marked/flagged as records in their metadata (see Appendix C for definition), so any version of a record can be recreated if needed.</td></tr>
<tr><td colspan="2"><b>Criterion 1.2:</b> The system assigns unique identifiers to records and their associated metadata. The system prevents any modification of a record's unique identifier once it is defined.</td></tr>
<tr><td><b>Sample Functions</b></td><td><b>Expected Results</b></td></tr>
<tr><td>Attempt to assign a common identification (ID) to two records.
Assign unique IDs to a set of records and their associated metadata. Check whether the IDs adhere to the records and their associated metadata.
Attempt to modify or delete assigned IDs.</td><td>The system notifies the user that a task is prohibited and prevents assignment of a common ID to two distinct records.
Assigned IDs adhere to the records and their associated metadata.
The system notifies the user that a task is prohibited and prevents modification and deletion of assigned IDs.</td></tr>
<tr><td colspan="2"><b>Criterion 1.3:</b> The system captures record metadata (FBI-designated and others) automatically and reliably links metadata to the records.</td></tr>
<tr><td><b>Sample Functions</b></td><td><b>Expected Results</b></td></tr>
<tr><td>Retrieve each of the designated metadata elements for a record.
Refer to Appendix E for the metadata list.</td><td>Each designated metadata element is retrieved and populated with a valid entry.
System captures all required metadata elements.</td></tr>
</table>

<table>
<tr><th colspan="2">2. CAPTURE RECORDS</th></tr>
<tr><td colspan="2"><b>Criterion 2.1:</b> The system imports records from sources outside the system (e.g., other information systems, desktop applications, scanned documents, or e-mail) along with all required associated metadata (e.g., records series, preexisting file plans [see Appendix C for definition] or locations for physical records)</td></tr>
<tr><td><b>Sample Function</b></td><td><b>Expected Results</b></td></tr>
<tr><td>Import a record and its associated metadata into the system from a desktop management system.</td><td>The record and its associated metadata are successfully imported into the system.</td></tr>
<tr><td colspan="2"><b>Criterion 2.2:</b> The system provides RM control over the records without physically transporting them to an RMA. The system links records to an external RMA.</td></tr>
<tr><td><b>Sample Function</b></td><td><b>Expected Result</b></td></tr>
<tr><td>Flag an entity in the system as a record and link it to the relevant file classification in the RMA.</td><td>The entity is identified in the system as a record and linked to the appropriate file classification and disposition in the RMA.</td></tr>
<tr><th colspan="2">3. MAINTAIN OR USE RECORDS
<i>3.1 Record Organization</i></th></tr>
<tr><td colspan="2"><b>Criterion 3.1.1:</b> The system accepts an FBI-specific scheme for organizing records. For example, the system accepts FBI-specific records disposition schedules and organizes records according to the schedules.</td></tr>
<tr><td><b>Sample Functions</b></td><td><b>Expected Results</b></td></tr>
<tr><td>Input an FBI-specific records disposition schedule into the system.
Input information declared as records with existing records disposition schedule characteristics.
Process and manage records in accordance with the records disposition schedule.</td><td>FBI-specific records disposition schedule is successfully input into the system.
Information input into the system is managed as records with correct records disposition schedule characteristics.</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Criterion 3.1.2:</b> Users can select categories (see Appendix C for definition) in which records are filed and assign records to these categories.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Input a user-designated file plan category.
Assign records to the user-designated file plan category.</td><td>User-designated file plan category conflicting with FBI-specific file plan is rejected.
User-designated file plan category that does not conflict with FBI-specific file plan is accepted.
Records assigned to the user-designated file plan category are contained within or linked to the category.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.3:</b> The system supports assignment of vital record (see Appendix C for definition) indicators.</td></tr>
<tr><th>Sample Functions</th><th>Expected Result</th></tr>
<tr><td>Input information known as a vital record.
Designate the information as a vital record by assigning a “yes” value to the vital record metadata element.</td><td>Record is shown as a vital record in its metadata.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.4:</b> If a vital record, system establishes a vital record review and update cycle.</td></tr>
<tr><th>Sample Function</th><th>Expected Result</th></tr>
<tr><td>The periodic replacement of obsolete copies of vital records with copies of current vital records. This may occur daily, weekly, quarterly, annually, or at other designated intervals, as specified by regulation or by RMAU.</td><td>Documentation indicating when the vital records update cycle occurs.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.5:</b> The system supports the linking of related records (e.g., a redacted record with its non-redacted counterpart, an original record with its revision, or an electronic record with a paper antecedent[4]).</td></tr>
<tr><th>Sample Function</th><th>Expected Result</th></tr>
<tr><td>Perform operation of linking records with other related records.</td><td>Record metadata carry information that designates other records to which they are linked.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.6:</b> The system supports the capability for users to create and edit file plans.</td></tr>
</table>

[4] For example, official correspondence may have been initiated on paper (paper antecedent), and the response was an electronic reply (electronic record).

<table>
<tr><td colspan="2">including categories and subcategories. The system prevents deletion of non-empty folders.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Create a system file plan and a category and subcategory within the file plan.
Edit the file plan, category, and subcategory.
Delete the file plan, category, and subcategory.
Attempt to delete a category containing items.</td><td>Categories and subcategories are successfully created, edited, and deleted in the system file plan.
The system notifies the user that this task is prohibited and prevents deletion of the category containing items.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.7:</b> The system can assign a status to records to prevent destruction (i.e., the system contains an indicator that includes an option to mark records as “do-not-destroy,” which prevents records from being selected for destruction or transfer according to records disposition schedules). When the reason for altering disposition has expired, it is necessary to unmark data.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Select the “do-not-destroy” status for a record that is identified for destruction according to the records disposition schedule.
Attempt to identify the record for destruction while the “do-not-destroy” status is selected.
Identify record folders and/or records that have been frozen and provide authorized individuals the capability to unfreeze them.</td><td>The “do-not-destroy” status is visible and enabled for the record.
Unsuccessful in identifying the record for destruction.
System should unfreeze records/record folders to the calculated phase of their life cycle as if they were never frozen.</td></tr>
<tr><td colspan="2"><b>Criterion 3.1.8:</b> The system supports global changes (see Appendix C for definition) to metadata, file plans, and records disposition schedules.</td></tr>
<tr><th>Sample Function</th><th>Expected Result</th></tr>
<tr><td>Change the value of a metadata element from its current value to another using keyed input.</td><td>All instances of the former value are changed to the new value. No instances of the former value remain in the selected metadata element.</td></tr>
</table>

Criterion 3.1.9: The system executes disposition (see Appendix C for definition) instructions (e.g., moves a group of records from active to inactive status or designates a group of records for destruction or transfer).

Sample Functions	Expected Results
Search the system for a set of records that are eligible for disposition.	System identifies and lists the set of records that are eligible for disposition.
Use authorized user ID to approve and execute the disposition instructions for the set of records.	The disposition instructions are successfully executed under the authorized user ID.
Use unauthorized user ID to attempt to approve and execute the disposition instructions for the set of records.	The system notifies the user that this task is prohibited and prevents the execution of disposition instructions under the unauthorized user ID.

Criterion 3.1.10: For systems that manage physical records, the system specifies identifiers for boxes, contents, locations, and the like. In other words, the system stores metadata for physical records not contained in the electronic information system and can identify physical records by physical location (e.g., box number, location ID, and similar).

Sample Function	Expected Result
Enter into the system physical location metadata for a physical record.	Metadata for the physical record is accepted and stored in the system.

Criterion 3.1.11: The record set of system documentation has been properly captured and uploaded to Sentinel in the 242 case file designated for this system.

Sample Function	Expected Result
Review the 242 case file to find which documents have been serialized for the record set of the system documentation.	Current system documentation has been properly captured within the 242 case file for the system.

3. Maintain or Use Records

3.2 Records Security

Criterion 3.2.1: The system prevents the overwriting of records. To comply with RM guidelines, records are never edited, but new versions are created and linked to the source.

Sample Functions	Expected Results
Copy a record from the system to a document management application (DMA).	Record copy is created and accessible in the document management system.
Modify the record and attempt to re-file it in the system.	System prevents the modified record from overwriting the original record. System prompts the user to file the modified record as a new record.

Criterion 3.2.2: The system prevents the deletion of indices, categories, and other "pointers" to records (i.e., it maintains referential integrity).	
Sample Function	**Expected Result**
User attempts to modify and/or delete indices and categories for a set of records.	Prohibited action does not happen. Indices or categories in use are not deleted or modified.
Criterion 3.2.3: The system (or system owner) maintains appropriate backup copies of records and recordkeeping systems.	
Sample Function	**Expected Result**
Confirm that backup procedures exist for the system.	The system follows its backup procedures and has evidence of being regularly backed-up.
Criterion 3.2.4: The system is protected by adequate recovery/rollback and rebuild procedures so that records may be recovered or restored following a system malfunction.	
Sample Function	**Expected Result**
Confirm that recovery/rollback and rebuild procedures exist for the system.	The system has recovery/rollback and rebuild procedures in place, and they have been tested.
3. MAINTAIN OR USE RECORDS ***3.3 Access & Retrieval***	
Criterion 3.3.1: The system controls access so that only authorized individuals are able to retrieve, view, print, copy, or edit records or other entities (e.g., metadata, file plan, etc.) in the recordkeeping system.	
Sample Functions	**Expected Results**
Designate a test set of user IDs; set access privileges to retrieve, view, print, copy or edit a record. Use an authorized user ID to retrieve, view, print, copy, or edit a record. Use an unauthorized user ID to attempt to retrieve, view, print, copy, or edit a record.	Record is able to be retrieved, viewed, printed, copied, and edited. The system notifies the user that these tasks are prohibited and prevents the actions from occurring.
Criterion 3.3.2: The system identifies individuals and groups of users and allows different access privileges to be assigned to individuals or groups. The system ensures that all access privileges (permissions and restrictions) are enforced on all retrievals.	
Sample Functions	**Expected Results**

Designate two test sets of user IDs; give members of each set different access privileges and restrictions. For each set of user IDs, attempt actions that are both allowable and restricted based on the access privileges and restrictions set. Designate a test set of user IDs; set different records retrieval access privileges for each of the IDs. With each user ID, attempt both allowable and prohibited retrievals.	Allowable actions occur for each set of user IDs. Prohibited actions do not occur for each set of user IDs Allowable retrievals occur. Prohibited retrievals do not occur.
Criterion 3.3.3: The system maintains the integrity of redacted records and ensures that redacted material is not accessible on sealed records (see Appendix C for definition).	
Sample Functions	**Expected Results**
Retrieve a random sample of sealed records and confirm that redacted material is not viewable. Attempt to reconstruct the redacted material.	All redacted material in the sealed records is not viewable. The redacted material cannot be reconstructed.
Criterion 3.3.4: The system provides a sufficiently wide range of search features and options, as needed to meet Bureau requirements. These might include searching on individual terms or a combination of terms; wildcard or exact-match searching, proximity or adjacency searching, relevance ranking of search results, use of stop words, limits on maximum size of results set from a search, query by image content, or others. See Appendix C for definitions of these terms.	

Sample Functions	Expected Results
Conduct records searches by: • Searching on individual terms. • Searching on a combination of terms. • Wildcard-matching. • Exact-matching. • Proximity or adjacency searching. • Excluding specified stop words. • Setting limits on the maximum size of the results set. • Searching image content. • Using other functions determined by system owner to be necessary for the system. Conduct a search that ranks the search results according to relevance (i.e., with the most relevant search results appearing at the beginning of the list and items gradually decreasing in relevance toward the bottom of the list).	All selected search functions are successfully completed. Search results include only those that match the search criteria. Search results are listed in order of relevance. System documentation describes the algorithm(s) used to rank search results.

3. Maintain or Use Records

3.4 Records Preservation

Criterion 3.4.1: The system enables migration of the records to a new format before the old format becomes obsolete. Any migration must be preplanned and controlled to ensure continued reliability of the records.

Sample Functions	Expected Results
Select a set of records and metadata. Convert a copy of the records to the standard FBI software format for migrating records.	The converted records and metadata are opened successfully in the new software format. The records and metadata content have not changed and remain readable and understandable.
Export a copy of records and metadata to another system and verify receipt of export.	The selected set of records and metadata is successfully imported to another system. The records and metadata content have not changed and remain readable and understandable.

<table>
<tr><td colspan="2"><b>Criterion 3.4.2:</b> The system ensures that captured metadata remains linked to the appropriate records without alteration throughout the life of the records.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Run sampling process on the upgrade copy to verify whether records remain associated with their metadata.
Run reporting function and output function.</td><td>Sample records are associated with their metadata.
Errors in associating records and metadata are reported and resolved prior to the migration of all data in the system.</td></tr>
<tr><th colspan="2">3. Maintain or Use Records
<i>3.5 Audit/Oversight</i></th></tr>
<tr><td colspan="2"><b>Criterion 3.5.1:</b> The system provides access to summary reports (e.g., number of accesses) and detail-level audit trail information (e.g., each individual record access, including record identifier, date, time, and user). The system supports the capability to continuously compile and output periodic and on-demand reports of summary and detailed audit trail information.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Set formats, data elements, parameters, and periodicity for audit trail reports.
Perform, output, and/or provide user access to periodic or on-demand audit trail reports.
Set system for continuous running of audit trail report function.</td><td>Periodic audit trail reports are successfully compiled and output according to set formats, data elements, parameters, and periodicity.
On-demand audit trail reports are successfully output and/or prepared for access.
System continuously runs the audit trail report function.</td></tr>
<tr><td colspan="2"><b>Criterion 3.5.2:</b> The system tracks failed attempts of all records activity and system functions. In other words, the system detects records and outputs any unsuccessful attempts to access records or metadata or conduct other system functions. The system tracks information such as user ID, date, and time of failed attempts.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Using an unauthorized user ID, attempt to modify a record.
Using an unauthorized user ID, attempt to modify user access permissions.</td><td>Failed attempt at record modification is detected, recorded, and output.
Failed attempt at modification of user access permissions is detected, recorded, and output.</td></tr>
<tr><td colspan="2"><b>Criterion 3.5.3:</b> Audit trail information is managed as records in order to prevent the editing of audit logs.</td></tr>
<tr><th>Sample Functions</th><th>Expected Results</th></tr>
<tr><td>Perform a set of actions resulting in audit trail activity.</td><td>Audit trail activity is recorded as expected.
Audit trail report is declared a record and its</td></tr>
</table>

Declare, either manually or automatically, the audit trail report a record, and enter associated metadata. Verify whether each audit trail report is declared a record with associated metadata.	associated metadata is linked to the record.
4. DISPOSE OF RECORDS (FINAL) (Transfer or Destroy)	
Criterion 4.1: The system identifies records eligible for transfer or destruction based on records disposition schedules and disposition instructions (i.e., the system automatically detects when a record's disposition period will pass, notifies RMAU that the record is eligible for disposition, and stipulates whether the record is eligible for transfer or destruction).	
Sample Functions	**Expected Results**
Develop a test set of records in the system that is eligible for disposition the following day.	RMAU is notified by the system that the set of records is eligible for disposition. RMAU is informed by the system regarding which records are eligible for transfer or destruction.
Criterion 4.2: The system exports records and metadata to be transferred (i.e., copies and subsequently removes them from the system) in a format acceptable for transfer to NARA.[5]	
Sample Functions	**Expected Results**
Verify whether in-system documentation records can be exported in NARA-accepted formats. Issue export command for a set of records.	Records are migrated and converted to an outside system or media in a NARA-acceptable format (only applicable to records that must be permanently retained).
Criterion 4.3: The system deletes records to be destroyed so that they cannot be physically reconstructed or otherwise retrieved.	
Sample Functions	**Expected Results**
Insert set of records and metadata to be destroyed. Issue destruction command for the records and metadata. Attempt to retrieve and reconstruct the records and metadata.	Designated records and metadata are deleted from the system. Neither the system nor any external procedures or software is successful in retrieving or reconstructing the records and metadata.
Criterion 4.4: The system maintains a record and provides certifiable proof of all transfers and destructions. All records of transfer or destruction are treated as records.	

[5] Contact NARA for acceptable transfer formats. See 36 CFR § 1228.270. Transfer formats are specified in records disposition schedules.

Sample Functions	Expected Results
Insert set of records and metadata to be destroyed. Issue destruction command for the records and metadata. Declare the fact of destruction of records and metadata to be a record for each member of set.	Records of destruction are maintained. Records of destruction are not capable of being destroyed.

5. Process Records Containing Restricted or National Security Classified Data

Criterion 5.1: The system captures national security classification metadata for classified records. These metadata elements include current classification, reason for (authority/the classification guide used), classification source, derivative source (if any), declassification date, downgrade instructions, review date, reviewer, declassification date, and declassifier.

Sample Functions	Expected Results
Import set of national security classified records to the system. Using an authorized user ID, enter metadata stipulating that the records are classified for purposes of national security, and populate additional classification-related metadata elements.	Imported national security classified records are accepted successfully in system with associated metadata. Metadata stipulating classification status, plus additional related metadata, are successfully entered in the system.

Criterion 5.2: For derivatively classified records, the system supports the capability to capture multiple reasons ("Reason(s) for Classification") and multiple sources ("Classified By") metadata elements.

Sample Functions	Expected Results
Import or designate a set of derivatively classified records. Assign multiple reasons and multiple sources in the associated metadata for each record.	Set of derivatively classified records is successfully designated or imported. Associated metadata for derivatively classified records successfully accepts multiple values for reasons and sources.

Criterion 5.3: The system provides a method for assigning classification levels to records (e.g., through a data or metadata field). The classification levels should include, but not be limited to: Confidential, Secret, Top Secret, and No Marking.

Sample Function	Expected Result
Enter five records, and assign a different classification level to each record.	Each record includes in its metadata a Confidential, Secret, Top Secret, or No Marking

	classification.
Criterion 5.4: The system provides a method for assigning the declassification review date.	
Sample Function	**Expected Results**
Indicate date on which the records should be reviewed under Executive Order (EO) 12958, as amended.	The date or the exemption category that applies to this set of records is successfully assigned.
Criterion 5.5: Authorized users can make changes to the retention period before declassification. [Note: Declassification review occurs outside the system.]	
Sample Function	**Expected Result**
Use an authorized user ID to modify the retention period for a set of records.	For the designated set of records, the retention period is successfully modified.
6. Interface with RMA (Export Records)	
Criterion 6.1: The system exports records and audit log history to the RMA.	
Sample Function	**Expected Results**
Issue a command to export a declared record and its history to the RMA.	The set of records and audit log history are successfully received by the RMA. The system no longer contains the exported set of records and metadata.
Criterion 6.2: The system exports metadata attached to records to the RMA.	
Sample Function	**Expected Results**
Issue command to export the metadata for a declared record to the RMA.	The set of metadata is successfully received by the RMA with the record. The system no longer contains the exported set of records and metadata.
Criterion 6.3: The system identifies and exports associated (linked) records and maintains record relationships.	
Sample Function	**Expected Results**
Select a test record that has associated records. Export the record to the RMA, indicating, if necessary, the transfer of any associated records.	The known associated records are transferred to the RMA. The relationship between the records is maintained in the RMA.
Criterion 6.4: The system supports the capability to add necessary metadata when records are exported.	

<table>
<tr><th>Sample Function</th><th>Expected Result</th></tr>
<tr><td>Access the metadata of an exported record from the sample test for criterion 6.2 and fill in missing fields.</td><td>Metadata file is accessed and missing metadata is successfully added.</td></tr>
<tr><td colspan="2"><b>Criterion 6.5:</b> The system maintains pointers to exported records (i.e., associated records in the system are linked to the exported record in the RMA). When a record is transferred from one system to another (the RMA), its "location" changes. Any pointers to the record in its old location need to be modified to reflect its new location.
For example, the system may contain past versions of a document (these versions may not be records, but documents), and the latest version is being transferred to a new RMA (possibly from a DMA). When a user opens up an outdated version of the document, the system should indicate that the latest version is located in the RMA.</td></tr>
<tr><th>Sample Functions</th><th>Expected Result(s)</th></tr>
<tr><td>Issue a command to export a record with associated records to the RMA.</td><td>Pointers in the system reflect the RMA identifier for the moved/exported record.</td></tr>
<tr><td colspan="2"><b>Criterion 6.6:</b> Unique identifiers are transferred from source systems to the RMA (i.e., the system sends the unique identifier for a record from the original system to the RMA when a record is transferred to the RMA).</td></tr>
<tr><th>Sample Functions</th><th>Expected Result(s)</th></tr>
<tr><td>Issue a command to export a record from the system to the RMA. In the RMA, check the status of the field for the original identifier.</td><td>The original system's correct unique identifier is located in the metadata of the record in the RMA.</td></tr>
</table>

Appendix E: Records Management Application Metadata List

System operations must be compared to this list of mandatory recordkeeping metadata elements. If an element is not required for the proper documentation and management of records due to the nature of system operations, the element should be indicated as "does not apply" during the RMAU evaluation of the system.

Element	Definition/Descriptions
Individual Documents	
Unique Record Identifier (may be system-generated)	An unambiguous system-generated data element that identifies a particular record.
Contributor Record ID	A unique ID, provided by the contributing system, that identifies a particular record within that system.
FBI Case Number	Identifies the classification, sub-classification (alpha), office of origin (OO), and sequential case number.
Serial	The number assigned to the document within the case.
Document Type	A code indicating the type of document. "TYPE" includes "DOCUMENT," "EMAIL," "IMAGE," etc.
Document Date	Generally, the date appearing on the face of the document. In the case of e-mail, it is the date the e-mail was sent.
To / Addressee	The recipient(s) of the document.
From / Author – Individual	The originator of the document. The individual who creates, sends, and signs the document.
From / Author – Organization	The organization to which the originator of the document belongs.
Title / Subject / Topic of Document	Generally, the "name" of the document (e.g., the title of an EC or memorandum, the subject line of an e-mail, the title of a report, briefing, or spreadsheet)
Description / Abstract / Notes	A brief narrative description of the record, which usually contains keywords.

Element	Definition/Descriptions
National Security Classification	Identifies the level of United States (U.S.) classified information. The document classification reflects the highest classification in the document.
Reason for National Security Classification	The authoritative source under which data is classified. For derivative classified records, the system must allow the listing of multiple authorities.
Declassification Review Date	When data is eligible for declassification.
Declassification Exemption Categories	Provide the capability for an authorized individual to enter or update exemption categories in the "Declassify On" field and optionally enter a declassification date or event that suppresses the "Declassify On" timeframe.
Other Restrictions	Identifies a record to which a legislative or regulatory restriction has been applied (e.g., Rule 6(e), Freedom of Information Act, or litigation matters).
Record Status	Indicates the distinction between the official record, a copy, duplicates, and similar items. The default would be "Records." Generally inherited from the file classification or file number.
Records Disposition	Actions taken with regard to federal records after they are no longer required to conduct current agency business. Generally inherited from the file classification or file number. Can be permanent, disposable, sample/select – undetermined, sample/select – permanent, sample/select – disposable, or unscheduled.
Selection Criteria	If the disposition is sample/select – permanent, this identifies the criteria used to make the retention determination.
Records Schedule Identification	Identification of the approved disposition authority. Generally linked from the file classification.

Element	Definition/Descriptions
Entry Date (may be system-generated)	The date the record was entered into the system.
Systems That Import and Manage E-Mail	
Address Name	E-mail sender; may be mapped to author or originator.
Distribution List	E-mail addressee; may be mapped to addressee(s) or other addressee(s).
Date/Time of Message Sent	E-mail date sent; may be copied as publication date.
Date/Time of Message Received	E-mail date received; may be mapped to date received.
Subject	E-mail subject may be mapped to subject and optionally as title.
Imported Records	
Scanned Image Format and Version	Possible formats: • Tagged Image Interchange Format (TIFF) 4.0 • TIFF 5.0 • TIFF 6.0 • Joint Photographic Experts Group (JPEG) (all versions) • Graphic Image Format (GIF) 87a • GIF 89a • Binary Image Interchange Format (BIIF) • Portable Network Graphics (PNG) 1.0
Portable Document Format (PDF) Version	Allowable versions are current or within two past versions.
Digital Photograph – Captions	Narrative text describing each individual image in order to understand and retrieve it. Standard caption information typically includes the who, what, when, where, and why about the photograph.

Element	Definition/Descriptions
Digital Photograph – Photographer	Identify the full name (rank) and organization (agency) of the photographer credited with the photograph.
Digital Photograph – Copyright	Indicate for each image whether there is a restriction on the use of the image because of a copyright or other intellectual property rights. The Bureau must provide, if applicable, the owner of the copyright and any conditions on the use of the photograph(s), such as start and end dates of the restrictions.
Digital Photograph – Bit Depth	Identify the bit depth of the transferred files.
Digital Photograph – Image Size	Specify the image height and width of each image in pixels.
Digital Photograph – Image Source	Identify the original medium used to capture the images.
Digital Photograph – Compression	Identify the file compression method used and the compression level (e.g., medium, high) selected for the image(s).
Digital Photograph – International Color Consortium/Image Color Management	Provide custom or generic color profiles, if available, for the digital camera or scanner used (e.g., standard red–green–blue [sRGB]).
Digital Photograph – Exchangeable Image File Format (EXIF) Information	Preserve and transfer to NARA the EXIF information embedded in the header of image files (as TIFF tags or JPEG markers) by certain digital cameras (e.g., make and model of the digital camera).
Web Records – File Name	The file name of each Web site file may not exceed 99ASCII (American Standard Code for Information Interchange) characters, and with the path the name it may not exceed 254 ASCII characters.
Web Records – Web Platform	Include the specific software applications and, where available, the intended browser applications and versions.
Web Records – Web Site Uniform Resource	Include the filename of the starting page of the

Element	Definition/Descriptions
Locator (URL)	transferred content.
Web Records – Capture Method	Include the name and description of harvester used. If PDF, include the software and version used to capture the PDF. If more than one method is used, clearly identify which content was captured by which method.
Web Records – Capture Date	Date record was captured.
Web Records – Contact	Point of contact (POC) information for person responsible for capturing the Web record.