INSTITUTE FOR DEFENSE ANALYSES

Rules to Navigate the Digital Highway: Information and Records Management for Data-Storage-as-a-Service and Migration to the Cloud

Laura A. Odell, *Project Leader*
Cameron E. DePuy
Laura R. Doolittle

November 2018

IDA Document
D-10353
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-4159, "WIN 10 SHB," for Director, Joint Service Provider. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Lee Kennedy

For more information:

Laura A. Odell, Project Leader
lodell@ida.org, 703-845-2009

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-10353

Rules to Navigate the Digital Highway: Information and Records Management for Data-Storage-as-a-Service and Migration to the Cloud

Laura A. Odell, *Project Leader*

Cameron E. DePuy

Laura R. Doolittle

Executive Summary

Organizations have two main drivers to store data: mission business needs and legal requirements. As data continues to accumulate and the investments required to buy, maintain, and operate storage devices grow; the business model for data storage is shifting. Cloud-based technologies are impacting the way data are being stored, retrieved, maintained, and preserved, creating opportunities for efficiencies if an organization can leverage these technologies while ensuring its data strategy meets records management requirements. Across the government, organizations must determine what has to be preserved, how long it has to be stored, and what constitutes an actual record. Total storage per year is trending higher, as many organizations lack deduplication policies and the rules regarding data preservation are not clearly defined.

OMB Circular No. A-130 states that "records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service."

This document is a guide to understanding the federal authorities for records management, the Executive Agencies' responsibilities, and the implications for the Department of Defense and the Joint Service Provider (JSP). As JSP transitions certain services to the cloud, there is an opportunity to incentivize customers to optimize their records management practices by allowing JSP to deduplicate data, eliminate old or untouched non-records, and ensure records are meeting the established storage schedules.

Contents

Figures

Tables

1. Why Do Organizations Store Data?

The amount of data being created is "doubling in size every two years, and by 2020 the digital universe – the data created and copied annually – will reach 44 zettabytes, or 44 trillion gigabytes."[1] As data continues to accumulate and the investments required to buy, maintain, and operate storage devices grow, the business model regarding data storage shifts. Corporate tracking reveals that their data grows 39% annually; however, over 40% of files have remained untouched for three years, and 12% have had no modification in seven years.[2]

Organizations store data to meet mission business needs and legal requirements. Organizations must take the appropriate action to protect the authenticity, reliability, integrity, and usability of records and identify requirements for their management to protect against potential legal and financial ramifications of deleting records, as well as the loss of productivity and data. Understanding what data is critical to the mission and what data is legally required to be saved are central to developing a data management strategy.

For the federal government, the National Archives and Records Administration (NARA) requires certain processes and time-based schedules for record keeping. Other industries have compliance standards they must abide to as well.

[1] EMC. The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. EMC White Paper. April 2014. Available at: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm [Accessed: September 9, 2017]

[2] http://datagenomicsproject.org/data-genomics-report-2016.html

Industry Snapshot: Financial Sector Legal Implications

The use of records management systems helps companies propose, apply, and develop policies and procedures that meet legal requirements. Non-compliance with regulations can lead to significant penalties. In the United States, the Sarbanes-Oxley Act is one of the most important record-management regulations, alongside the Gramm-Leach-Bliley Act and others. The Sarbanes-Oxley Act emerged in 2002 as the response to the financial scandals of large multinationals, which put the credibility of the accounting and auditing systems in check. This law:

- Stipulates that the finance directors and executive directors of companies must personally certify the financial records and offer related information periodically.
- Establishes guidelines for audit committees.
- Obligates the retention of any relevant document control in the framework of government investigations.

Failure to comply with these and other regulations could result in penalties. Another legal principle present in the Sarbanes-Oxley Act is that of *spoil*. "The exploitation holder – it is understood by such activities leading to the destruction or alteration of records – determines that any evidence will be taken as evidence against the spoiler or offender. Therefore, any damage, change (falsification) or error in the preservation of records, can be used against the organization in litigation and consequently be subject to penalties." Close scrutiny of corporate governance and greater responsibility placed on directors to vouch for the reports, have resulted in the growth of software solutions aimed at reducing the complexity, time, and expense involved in creating the reports. The consequence of this legal framework exemplifies the importance of a record management system.

2. What Are the Federal Authorities Surrounding Records Management?

U.S. Code 44 Chapter 21 designates NARA as the authoritative agency that preserves and documents government and historical records.[3] The objectives of records management include accurate documentation of policies and transactions of the federal government, control of the quality of records, prevention of the creation of unnecessary records, simplification of the systems and process of records creation, as well as judicious preservation and disposal of records.[4]

Records are defined in various statutes, including the Federal Records Act. The Federal Records Act governs federal government agencies' records management responsibilities. It defines records as all, "books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical 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 Government or because of the informational value of the data in them."[5]

The Code of Federal Regulations (CFR) defines "non-record materials" to include material such as unofficial copies of documents kept only for convenience or reference, stocks of publications and near-print documents, and library or museum material intended solely for reference or exhibition.

U.S. Code 44 Chapter 33 states that government agencies are required to establish records management programs in which a relationship is established with the Archivist of the United States to promote the preservation of those records deemed appropriate for preservation, and the destruction of records of only temporary value.

Under those authorities for NARA, the Archivist of the United States issues General Records Schedules (GRS) that authorize, after specified periods of time, the destruction of temporary records or the transfer to the National Archives of the United States of permanent

[3] https://www.archives.gov/faqs

[4] Title 44 Chapter 29

[5] https://www.archives.gov/records-mgmt/faqs/federal.html

records. An example of an email schedule is displayed in Table 2-1. Further GRS schedules may be found in Appendix A.

Table 2-1. Example Email Schedule

Description	Disposition Instructions	Time Frame / Notes	Exceptions
Email Managed under a Capstone Approach (GRS 6.1)			
Email of Capstone Officials	PERMANENT – TRANSFER	Transfer to NARA after 15-25 years or after declassification review	No
Email of Non-Capstone Officials – All others except below	TEMPORARY-DELETE	7 YEARS	Yes - longer retention authorized if needed for business use.
Email of Non-Capstone Officials – Support and/or administrative positions	TEMPORARY-DELETE	3 YEARS	Yes – longer retention authorized if needed for business use.

The Government Records Directive also lays out the next generation of federal records management compliance. By 2019, all public sector organizations will have to manage their permanent records electronically. By 2022, NARA will no longer accept any federal records into their archives in physical format, and agencies will be responsible for submitting only digitized content.[6]

NARA's Universal Electronic Records Management (ERM) requirements are derived from existing NARA regulations, policy, and guidance. ERM applications provide the business logic required to capture, control, maintain, and dispose of electronic records. They allow the user to declare electronic files as records and associate them to a file code and corresponding disposition authority.[7] Figure 2-1 details the operational activities that provide the criteria for successfully managing permanent electronic records according to NARA.

[6] https://www.archives.gov/records-mgmt/prmd.html

[7] https://www.archives.gov/records-mgmt/policy/requirements-guidance.html#erm-app

Figure 2-1. Electronic Records Management

3. What Are the Executive Agency's Responsibilities?

To carry out the regulations from NARA and guidance from the GRS, the heads of executive agencies establish continuing programs for efficient and economical management of records and must integrate recordkeeping and record disposal practices into agency processes. Agencies must develop records schedules for all records created and received by the agency and receive NARA approval for those schedules prior to implementing them. Agencies are responsible for distinguishing between records and non-record materials by applying the relevant definitions.[8] Records must not be destroyed except under the provisions of NARA-approved agency records schedules or the General Records Schedules issued by NARA.

A November 2011 Presidential Memorandum on Managing Government Records directed the establishment of a single framework for agencies to follow for managing federal records. Subsequently, the Office of Management and Budget (OMB) and NARA issued the Managing Government Records Directive, which defines this framework. The framework guidance stated that all agencies must name a Senior Agency Official for Records Management (SAORMs) by November 2012.[9] SAORMs act on behalf of the agency head to ensure the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy, and OMB policy.

OMB Circular No. A-130 includes a basic consideration that, "systematic attention to the management of Federal Government records from creation to disposition is an essential component of sound information resources management that promotes public accountability." It states that agencies shall:

- Designate a SAORM who has overall agency-wide responsibility for records management;
- Institute records management programs that provide documentation of agency activities;
- Manage electronic records in accordance with government-wide requirements.
- Ensure the ability to access, retrieve, and manage records throughout their life cycle regardless of form or medium;

[8] https://www.archives.gov/files/records-mgmt/rm-glossary-of-terms.pdf

[9] https://records-express.blogs.archives.gov/2012/08/24/records-management-directive-released/

- Ensure agency records managed by the SAORM are treated as information resources and follow the requirements in this Circular;
- Establish and obtain the approval of the Archivist of the United States for retention schedules for federal records in a timely fashion;
- Ensure the proper and timely disposition of federal records in accordance with a retention schedule approved by the Archivist of the United States; and
- Provide training and guidance, as appropriate, to all agency employees and contractors regarding their federal records management responsibilities[10]

SAORMs serve as an executive sponsor with broad responsibility for the agency records management program. The incumbents primarily operate at the strategic level to establish an agency records management program's vision, goals, and objectives in alignment with NARA and agency-specific strategic plans. SAORMs ensure their records management programs receive adequate resources to complete their mission. In addition, Agency Records Officers manage and implement agency records management programs. Their focus is primarily operational, ensuring that the agency is in compliance with the foundational requirements for records management. Agency Records Officers work closely with NARA and serve as records management advisors to SAORMs.[11] The SAORM bridges the gap between the agency head and the Agency Records Officer in order to provide strategic direction for the agency's records management program.[12] SAORMs are required by the joint OMB/NARA-issued Managing Government Records Directive (M-12-18) and the NARA Bulletin 2017-02 to report to NARA on agency progress in meeting the Directive goals and on other significant records and information management initiatives as defined by NARA.[13] Details of SAORM and Records Officer responsibilities may be found in Appendix B.

[10]https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[11] https://records-express.blogs.archives.gov/2018/03/12/roles-and-responsibilities-for-records-management-programs/

[12] https://www.archives.gov/records-mgmt/agency/sao-list

[13] https://www.archives.gov/files/records-mgmt/agency/dod-saorm-2017.pdf

4. Implications for the Department of Defense (DoD)?

In 2017, the DoD Chief Information Officer (CIO) updated Department of Defense Instruction (DoDI) 5015.02 "Records Management Program." The instruction is the basis for records management policy within the DoD. It establishes policy and assigns responsibilities for the management of DoD records in all media, including electronic media.[14] The responsibilities of the DoD CIO include the development and establishment of DoD policy and standards to implement a DoD Records Management Program. The DoD CIO, specifically the Deputy CIO for Resources and Analysis, serves as the DoD SAORM. They submit an annual report to NARA detailing the agency-wide strategy and progress in meeting all requirements, as required by OMB/NARA Managing Government Records Directive (M-12-18). The DoD CIO appoints DoD Records Officers to guide and coordinate the DoD Records Management Program throughout the Department. The DoD CIO also provides required records management training to educate DoD personnel on their records management responsibilities in accordance with NARA Bulletin 2017-01.

DoD Records Officers collaborate with DoD Components and NARA to execute the DoD Records Management Program. The OSD Records and Information Management Program (RIM) has oversight over OSD and support Defense Agencies and Field Agencies to maintain and update the Records Disposition Schedules[15]. Agencies may also put out their own guidance. For example, Defense Information Systems Agency (DISA) Instruction 210_15_6 "Records Management" prescribes policy and assigns responsibilities for records management within DISA. It also advises of the penalties, exceptions for, and required documentation of the destruction of federal records. Records management for DISA ensures the creation and preservation of adequate and proper documentation of the DISA organization, functions, policies, decisions, procedures, and essential transactions.[16]

[14] http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501502p.pdf

[15] Records Disposition schedules may be found at: http://www.esd.whs.mil/RIM/

[16] https://www.disa.mil/-/media/Files/DISA/About/Publication/Instruction/di210156.pdf

5. What Does This Mean for the Joint Service Provider?

JSP is responsible for storing and managing all data, including record and non-record material, for the National Capital Region (NCR), including the Pentagon. As a field activity under DISA, JSP should fall under DISA's records management program. However, the data that JSP stores for customers such as the Office of Cost Assessment and Program Evaluation (CAPE), have their own record schedules and Records Officers. Those organizations have the responsibility of designating, or tagging, which data are considered records and must be stored or kept. Many organizations have developed record schedules but do not yet closely evaluate their data, creating a tendency to overstore non-record material. Within the NCR/Pentagon, the H drive, or personal drive has 472 TBs of aggregate storage; the O drive,

Industry Snapshot: Redundant, Obsolete, Trivial Data

Industry is finding redundant, obsolete, and trivial data (ROT); this is identified as data with little or no business value. At least 30% of data is identified as ROT (*Veritas, The State of Information Management: United States of America*). Organizations need an IT policy that states when ROT data will be deleted. Figure 5-1 identifies the increased level of cash flow when organization have a continual IT policy stating when ROT data needs to be deleted.

Although ROT is a common issue in data management, industry has determined methods to manage their records such as deduplication and specific deletion schedules.

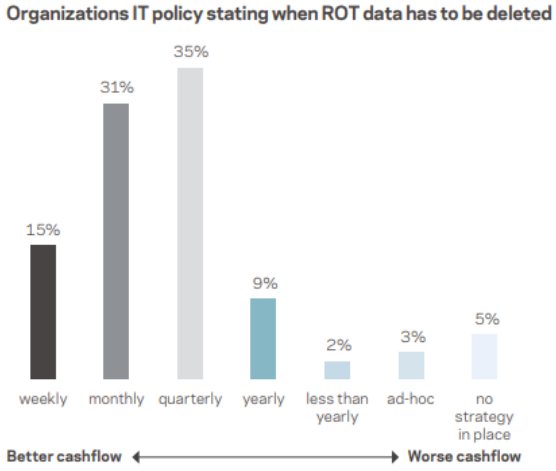

Figure 5-1. ROT Data Deletion Policy and Cash flow

or organizational drive, has 1.2 PBs of aggregate storage; and .pst data has 287 TBs of aggregate storage.

OMB Circular No. A-130 states that "records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service." As JSP transitions certain services to the cloud, there is an opportunity to push customers to enforce records management, allowing JSP to deduplicate data, eliminate old or untouched non-records, and ensure records are meeting the established storage schedules.

Appendix A. NARA General Records Schedule

NARA Transmittal 29 is the most recent revision of the GRS. Based on this revision of the GRS, the IDA research team pulled relevant details regarding retention and disposition for records types applicable to the scope of the sponsor's task, including disposition instructions with time retention, possible exclusions or exceptions, and the disposition authorities. Records identified as relevant were categorized under the GRS Section 3, Technology, Section 4, Information Management, Section 5, General Operations Support, and Section 6, Mission Support. Table A-1 captures this analysis.

Table A-1. National Archives and Records Administration. (2017). *Transmittal 29 General Records Schedule*.

Description	Disposition Instructions	Time Frame / Notes	Exceptions
General Technology Management Records (GRS 3.1)			
Technology management administrative records	TEMPORARY – DESTROY	5 YEARS	Yes – longer retention authorized if needed for business use. Does not apply to CIO records.
Infrastructure project records	TEMPORARY – DESTROY	5 YEARS (after project is terminated)	Yes – longer retention authorized if needed for business use. Does not apply to records relating to specific systems that support or document mission goals.
System development records	TEMPORARY – DESTROY	5 YEARS (after system is superseded, terminated, defunded, or defunct)	Yes – longer retention authorized if needed for business use. Does not apply to system data or content.
Special purpose computer programs and applications	TEMPORARY – DELETE	(when related master file or database has been deleted)	Yes – longer retention authorized if needed for business use. Does not apply to software or applications necessary to maintain unscheduled master files or databases, databases scheduled to National Archives, or

Description	Disposition Instructions	Time Frame / Notes	Exceptions
			commercial-off-the-shelf software.
Information technology operations and maintenance records	TEMPORARY – DESTROY	3 YEARS (after agreement, control measures, etc. is completed, terminated or superseded.	Yes – longer retention authorized if needed for business use.
Information technology oversight and compliance records	TEMPORARY – DESTROY	5 YEARS (after project is completed)	Yes – longer retention authorized if needed for business use.
Documentation necessary for preservation of permanent electronic records	PERMANENT – TRANSFER	N/A	Yes – agencies may retain a copy of documentation and can destroy AFTER original has been transferred to National Archives.
All documentation for temporary electronic records and documentation not necessary for preservation of permanent records	TEMPORARY – DESTROY	5 YEARS (after project is completed)	Yes – longer retention authorized if needed for business use.
Information Systems Security Records (GRS 3.2)			
Systems and data security records	TEMPORARY – DESTROY	1 YEAR(s) (after system is defunct or no longer needed for continuity of security controls)	No.
Computer security incident handling, reporting and follow-up records	TEMPORARY – DESTROY	3 YEARS	Yes – longer retention authorized if needed for business use.
Systems not requiring special accountability for access	TEMPORARY – DESTROY	When all business use ceases	Yes – excludes records relating to electronic signatures and/or monitoring for mission activities.
Systems requiring special accountability for access	TEMPORARY – DESTROY	6 YEARS (after account is altered or terminated)	Yes – longer retention authorized if needed for business use.
Systems backups and tape library records – Incremental backup files	TEMPORARY – DESTROY	When superseded by a full backup, or when no longer needed for system restoration, whichever is later	No.

Description	Disposition Instructions	Time Frame / Notes	Exceptions
Systems backups and tape library records – Full backup files	TEMPORARY – DESTROY	When subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later	No.
Backups of master files and databases – File identical to permanent records scheduled for transfer to the National Archives	TEMPORARY – DESTROY	Immediately after the identical records have been captured in a subsequent backup file or when original has been transferred to National Archives	Yes – longer retention authorized if needed for business use.
Backups of master files and databases – File identical to temporary records authorized for destruction by a NARA-approved records schedule	TEMPORARY - DESTROY	Immediately after the identical records have been deleted or replaced by a subsequent backup file	Yes – longer retention authorized if needed for business use.
Records Management Records (GRS 4.1)			
Records management program records	TEMPORARY – DESTROY	6+ YEARS (no sooner than 6 years after the project is completed)	Yes – longer retention authorized if needed for business use. Does not apply to copies maintained by NARA.
Vital or essential records program records	TEMPORARY – DESTROY	3 YEARS (after project is completed)	Yes – longer retention authorized if needed for business use.
Copies of vital records	TEMPORARY – DESTROY	When superseded by the next cycle	No.
Forms of management records	TEMPORARY – DESTROY	3 YEARS (after form is cancelled)	Yes – longer retention authorized if needed for business use.
Freedom of Information Act (FOIA), Privacy Act, and classified documents administrative records	TEMPORARY – DESTROY	3 YEARS	Yes – longer retention authorized if needed for business use. Does not cover records documenting policies and procedures accumulated in offices having agency-wide responsibilities for FOIA, Privacy Act, and classified documents.

Description	Disposition Instructions	Time Frame / Notes	Exceptions
General information request files	TEMPORARY – DESTROY	90 DAYS	Yes – longer retention authorized if needed for business use.
Access and disclosure request files	TEMPORARY – DESTROY	6 YEARS (after final agency action) OR 3 YEARS (after final adjudication by courts) Whichever is later	Yes – longer retention authorized if needed for business use.
Information access and protection operational records – Information access and protection tracking and control records	TEMPORARY – DESTROY	2 YEARS (after last entry, when associated documents are declassified or destroyed or when authorization expires)	Yes – longer retention authorized if needed for business use.
Information access and protection operational records – Access control records	TEMPORARY – DESTROY	When superseded or obsolete	Yes – longer retention authorized if needed for business use.
Information access and protection operational records – Records relating to classified or controlled unclassified document containers	TEMPORARY – DESTROY	90 DAYS (after last entry)	Yes – longer retention authorized if needed for business use.
Agency reports to the Congress, Department of Justice, or other entities regarding FOIA, Mandatory Declassification Review (MDR), Privacy Act, and similar access and disclosure programs	TEMPOARY – DESTROY	2 YEARS (after date of report)	Yes – longer retention authorized if needed for business use. Does not apply to summary reports incorporating government-wide statistics.
Automatic and systematic declassification review program needs	TEMPORARY – DESTROY/DELETE	30 YEARS (after review completion)	Yes – longer retention authorized if needed for business use.
Fundamental classification guidance review files	TEMPORARY – DESTROY	5 YEARS	Yes – longer retention authorized if needed for business use.

Description	Disposition Instructions	Time Frame / Notes	Exceptions
		(after report submission to Information Security Oversight Office (ISOO))	
Classified information nondisclosure agreements – records maintained in the individual's official personnel folder	N/A – Applies the disposition for the official personnel folder	N/A	N/A
Classified information nondisclosure agreements – records maintained separately from the individual's personnel folder	TEMPORARY – DESTROY	50 YEARS	No.
Personally identifiable information extracts	TEMPORARY – DESTROY	90 DAYS (or when no longer needed pursuant to supervisory authorization)	No.
Personally identifiable information extract logs	TEMPORARY – DESTROY	When business use ceases	No.
Privacy Act System of Records Notices (SORNs)	TEMPORARY – DESTROY	2 YEARS (after supersession by a revised SORN or after system ceases operation)	Yes – longer retention authorized if needed for business use.
Records analyzing PII – Records of Privacy Threshold Analyses (PTAs) and Initial Privacy Assessments (IPAs)	TEMPORARY – DESTROY	3 YEARS (after associated Privacy Impact Assessment (PIA) is published or determined unnecessary)	Yes – longer retention authorized if needed for business use.
Records analyzing PII – Records of PIAs	TEMPORARY – DESTROY	3 YEARS (after superseding PIA is published, after system ceases operation, or after website is no longer available to public)	Yes – longer retention authorized if needed for business use.
Common Office Records (GRS 5.1)			
Administrative records maintained in any agency office	TEMPORARY – DESTROY	When business use ceases	Yes – does not apply to recordkeeping copies of organizational charts, functional statements, and related records that

Description	Disposition Instructions	Time Frame / Notes	Exceptions
			document mission-related organization, staffing, and procedures of the office.
Non-recordkeeping copies of electronic records	TEMPORARY – DESTROY	Immediately after copying to a recordkeeping system or otherwise preserving	Yes – longer retention authorized if needed for business use.
Records of non-mission related internal agency committees	TEMPORARY – DESTROY	When business use ceases	Yes – does not cover records of FACA or interagency committees.
Continuity and Emergency Planning Records (GRS 5.3)			
Continuity planning and related emergency planning files	TEMPORARY – DESTROY	3 YEARS (or 3 years after superseded or obsolete)	Yes – longer retention authorized if needed for business use. Does not include incident response records, high-level government-wide Continuity of Government (COG) records, or high-level officials (capstones).
Employee emergency contact information	TEMPORARY – DESTROY	When superseded, obsolete, or when employee separates or transfers employment	Yes – does not include employee directories.
Mail, Printing, and Telecommunication Service Management Records (GRS 5.5)			
Mail, printing, and telecommunication services administrative and operational records	TEMPORARY – DESTROY	3 YEARS	Yes – longer retention authorized if needed for business use. Excludes agreements for voucher payment.
Mail, printing, and telecommunication services control records	TEMPORARY – DESTROY	1 YEAR (or when superseded or obsolete)	Yes – longer retention authorized if needed for business use. Excludes USPS records tracking shipment, reports of loss, requisitions used to support payment, or mailing lists.
Security Records (GRS 5.6)			
Security administrative records	TEMPORARY – DESTROY	3 YEARS	Yes – longer retention authorized if needed for business use.
Records of routine security operations	TEMPORARY – DESTROY	30 DAYS	Yes – longer retention authorized if needed for business use. Excludes

Description	Disposition Instructions	Time Frame / Notes	Exceptions
			law enforcement officer-related records.
Accident and incident records	TEMPORARY - DESTROY	3 YEARS (after final investigation or reporting action)	Yes – longer retention authorized if needed for business use.
Information security violations records	TEMPORARY – DESTROY	5 YEARS (after close of case or final action)	Yes – longer retention authorized if needed for business use. Excludes documents used for official personnel folder or records of subsequent investigations.
Insider threat administrative and operations records	TEMPORARY – DESTROY	7 YEARS	Yes – longer retention authorized if needed for business use.
Insider threat inquiry records	TEMPORARY – DESTROY	25 YEARS	Yes – longer retention authorized if needed for business use. Excludes records of any subsequent investigations.
Insider threat information	TEMPORARY – DESTROY	25 YEARS	Yes – longer retention authorized if needed for business use. Excludes case files of any subsequent investigations.
Agency Accountability Records (GRS 5.7)			
Internal administrative accountability and operational management control records	TEMPORARY – DESTROY	1 YEAR	Yes – longer retention authorized if needed for business use. Excludes reports related to agency mission activities, consolidated final agency reports submitted to the President/OMB or Congress, or reports that mandating agencies receive.
Internal control review, response, and mitigation management records	TEMPORARY – DESTROY	5 YEARS (after no further corrective action is needed)	Yes – longer retention authorized if needed for business use. Excludes records used for internal review.

Description	Disposition Instructions	Time Frame / Notes	Exceptions
Administrative directives and notices	TEMPORARY – DESTROY	When superseded or obsolete	Yes – excludes documents related to mission activities.
Records about authorizing and managing report requirements and parameters	TEMPORARY – DESTROY	2 YEARS	Yes – longer retention authorized if needed for business use.
Mandatory reports to external federal entities regarding administrative matters	TEMPORARY – DESTROY	6 YEARS (after report submission or after oversight approval)	Yes – longer retention authorized if needed for business use. Excludes reports on finance matters or if oversight entities request separate schedule.
Administrative Help Desk Records (GRS 5.8)			
Technical and administrative help desk operational needs	TEMPORARY – DESTROY	1 YEAR	Yes – excludes public customer service records under GRS 6.5.
Email Managed under a Capstone Approach (GRS 6.1)			
Email of Capstone Officials	PERMANENT - TRANSFER	Transfer to NARA after 15-25 years or after declassification review	No.
Email of non-Capstone Officials – All others except below	TEMPORARY – DELETE	7 YEARS	Yes – longer retention authorized if needed for business use.
Email of non-Capstone Officials – Support and/or administrative positions	TEMPORARY – DELETE	3 YEARS	Yes – longer retention authorized if needed for business use.
Information Technology Records (GRS 6.3)			
Information technology program and capital investment planning records	TEMPORARY – DESTROY	7 YEARS	Yes – longer retention authorized if needed for business use. Excludes policy records generated by CIO, records of government-wide committees sponsored by CIOs, system data or content, systems development records, or records documenting system and operational level compliance with IT

Description	Disposition Instructions	Time Frame / Notes	Exceptions
			policies, directives, and plans.
Enterprise architecture (EA) records	TEMPORARY – DESTROY	7 YEARS (after creating a new iteration of the EA or Information Assurance (IA))	Yes – longer retention authorized if needed for business use.
Public Affairs Records (GRS 6.4)			
Public affairs-related routine operational records	TEMPORARY – DESTROY	3 YEARS (or when no longer needed, whichever is later)	No.
Public correspondence and communications not requiring formal action	TEMPORARY – DESTROY	90 DAYS	Yes – longer retention authorized if needed for business use. Excludes correspondence relating to a specific case of action that is not considered public or public comments that an agency takes action on or uses to take action.
Public affairs product production files	TEMPORARY – DESTROY	When no longer needed	Yes – excludes final products, unique collections of products or original material the agency assembles for research or final product development purposes, working papers or files, bibliographies, checklists, indexes relating to records scheduled as permanent, etc.
Routine media relation records	TEMPORARY – DESTROY	When no longer needed	Yes – excludes transcripts of press conferences or briefings, briefing books, and press releases not covered by this item.

Note: Retrieved from https://www.archives.gov/files/records-mgmt/grs/grs-trs29.pdf

Appendix B. SAORM and Records Officer Principal Duties and Responsibilities[17]

SAORM	Agency Records Officer
Provides agencies with a clear vision and strategic direction to modernize agency records management program(s).	Interprets and advises senior agency officials on existing, new, or potential records management statutes, regulations, or other legal requirements impacting the agency. May also be responsible for strategic direction in micro agencies.
Ensures adequate records management resources are embedded into the agency's Strategic Information Resources Management Plan.	Integrates records management and archival requirements into the design, development, and implementation of electronic information systems.
Provides adequate budgetary and personnel resources to implement an efficient and effective agency records management program.	Works with internal stakeholders to identify budgetary, personnel, and system requirements. Participates in the Capital Planning and Investment Control process.
Establishes, where appropriate, agency-level records management program offices to ensure adequate management of routine mission support functions.	Manages department-level and/or agency-level records management program office(s). Routine mission functions may include the transfer of permanent records to NARA, records storage and retrieval, development and update of records schedules, management of litigation holds or records freezes, and administration of internal program evaluations, including performance measurements where possible.
Ensures the designation of records management responsibilities in each program (mission area) and administrative area to ensure the incorporation of record-keeping requirements and records maintenance, storage, and disposition practices into agency programs, processes, systems, and procedures.	Implements and assesses each program area's record-keeping practices, including but not limited to records maintenance, storage, and disposition practices into agency programs, processes, systems, and procedures.

[17] https://records-express.blogs.archives.gov/2018/03/12/roles-and-responsibilities-for-records-management-programs/

SAORM	Agency Records Officer
Ensures agency staff are informed of and receive training on their records management responsibilities.	Develops and administers agency-wide records management training. See NARA Bulletin 2017-02.
Issues agency directives, policies, and initiatives supporting OMB and NARA Directive goals and subsequent guidance for transitioning toward a fully electronic government.	Carries out records management modernization initiatives resulting from new records management directives, policies, or standards.
Ensures agency compliance with NARA requirements for electronic records, including the electronic management of all permanent electronic records to the fullest extent possible for eventual transfer and accessioning by NARA.	Monitors and reports compliance with NARA and agency-specific requirements for the management and transfer of permanent electronic records.
Directs agency efforts across program areas to ensure email records are managed electronically and retained in an appropriate electronic information system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records consistent with NARA-approved disposition authorities and regulatory exceptions.	Establishes procedures and guidance for email records. Coordinates with IT to ensure systems adhere to records management retention and disposition policies.
Ensures policies, procedures, and systems are in place and configured to protect records against unauthorized removal or loss.	Coordinates with IT to ensure records management considerations for systems access and security controls are implemented. Participates in agency reporting processes involving unauthorized removal or loss of records and formally notifies NARA.
Directs the use of agency-wide records management internal controls, self-assessments, and remediation plans.	Implements agency-wide records management internal controls to ensure records, regardless of format or medium, are properly organized, classified or indexed, and made available for use. Oversees self-assessment and remediation activities.
Reviews NARA's annual Records Management Self-Assessment analysis and risk ratings to determine vulnerabilities and identify plans for improvement.	Supports SAORMS and/or leads in gathering data and developing responses to NARA's oversight and reporting activities.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-11-18	Final	

4. TITLE AND SUBTITLE

Rules to Navigate the Digital Highway—Information and Records Management for Data-Storage-as-a-Service and Migration to the Cloud

5a. CONTRACT NUMBER

HQ0034-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)

Cameron E. DePuy, Laura R. Doolittle

5d. PROJECT NUMBER

BC-5-4159

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

D-10353

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Maj Gen Brian Dravis
Director, Joint Service Provider
Pentagon

10. SPONSOR'S / MONITOR'S ACRONYM

JSP

11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Laura A. Odell

14. ABSTRACT

Organizations have two main drivers to store data: mission business needs and legal requirements. As data continues to accumulate and the investments required to buy, maintain, and operate storage devices grows; the business model regarding data storage is shifting. Cloud based technologies are impacting the way data is being stored, retrieved, maintained, and preserved creating opportunities for efficiencies if an organization can leverage these technologies while ensuring its data strategy meets records management requirements. Across the government, organizations must determine what has to be preserved, how long it has to be stored, and what constitutes an actual record. Total storage per year is trending higher, as many organizations lack deduplication policies and the rules regarding data preservation are not clearly defined. This paper outlines specific steps the government can take to optimize data management by: complying legal and government policy, applying industry best practice, and utilizing technologies.

15. SUBJECT TERMS

data storage-as-a-service, records and information management, controlled unclassified information

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Maj Gen Brian Dravis
Unclassified	Unclassified	Unclassified	Unlimited	23	19b. TELEPHONE NUMBER (Include Area Code) 703-697-8112