WHITE PAPER

Addressing Archiving and Retention Challenges In the Government Sector

By Heidi Biggar
With Brian Babineau

March, 2008

Table of Contents

Introduction

Today's record retention laws were born out of the system of check and balances that has been in place for legislation for years. When legislation is drafted by a governing body, records are kept on who supported the law, the date the legislation was enacted, etc. Following this example, regulatory bodies, such as the Securities and Exchange Commission (U.S.) and the Financial Services Administration (U.K.), have built record creation and retention rules into their own laws. The irony is that while the majority of industry regulatory bodies have adapted their retention laws to include electronic records—such as e-mail—this process is still evolving at many government agencies. Since the majority of documents today are created electronically, government agencies find themselves in the challenging position of having to find way to comply with regulations.

Compounding the IT burden for government organizations is huge data growth. As more and more agencies shift from paper to digital (or electronic) operations, the IT burden grows. Factor in longer retention periods and the IT burden gets that much greater. Just consider the IT impact of backing up more information and replicating it for DR purposes.

Government organizations must also deal with the unique access challenges of the data they store. Birth certificates, contributions to political campaigns, maps of enemy territory, etc. are examples of government records with varying access requirements. IT organizations must find ways to balance the cost of storing this data while meeting data availability (or access) requirements. Additionally, many government records contain classified and highly confidential information. These records have to be properly secured throughout their lifetime (i.e., for the period of time they are stored).

As government organizations look to solve some of the storage, data protection and security challenges posed by regulatory compliance, discussions about archiving information in a tiered environment (i.e., on multi-tiered storage platform) are certain to take place. Many private sector companies are using a combination of disk and tape systems to meet their storage requirements. Doing so allows them to save information for extended periods of time while maintaining appropriate levels of accessibility and cost. In some cases, this requires customers to buy multiple storage hardware and software solutions—and move data back and forth among these resources.

The IBM System Storage DR550 makes this process much easier and cost-effective, allowing users to scale capacity by adding either disk or tape (or even optical) as needed within a single system based on data requirements. This paper looks at the capabilities of the DR550, which make it an ideal platform to address the compliance issues of government agencies. It also looks at some of the specific mandates and how organizations must deal with information retention and security issues going forward.

Government Regulations

NARA's Role

Almost every government organization and agency has to create and retain records. In fact, there are so many rules that it would be impossible to cover them all in this paper. This paper looks at a few examples, starting with those imposed by the U.S. National Archives and Records Administration (NARA).

NARA was established to determine what types of documents federal agencies must keep. NARA's establishment and rules (impact how government records are generated, transported and stored) (Figure 1).

FIGURE 1. SELECT TITLES AND SECTIONS FROM THE UNITED STATES CODE AS ITS RELATES TO NARA AND THE ESTABLISHMENT OF FEDERAL RECORDS MANAGEMENT PROGRAMS

Regulation	Applicable Section Titles / Descriptions
44 United States Code (U.S.C.) Chapter 21 Subsection 2102[1]	Establishment. There shall be an independent establishment in the executive branch of the Government to be known as the National Archives and Records Administration. The Administration shall be administered under the supervision and direction of the Archivist.
44 U.S.C. Chapter 31 Subsection 3101[2] (Federal Records Act)	Records management by agency heads; general duties. The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.
36 CFR Sec. 1220.1[3]	Responsibility for records management programs. The National Archives and Records Administration Act of 1984 amended the records management statutes to divide records management responsibilities between the National Archives and Records Administration (NARA) and the General Services Administration (GSA). Under the Act, NARA is responsible for adequacy of documentation and records disposition and GSA is responsible for economy and efficiency in records management. NARA regulations are codified in this subchapter. GSA records management regulations are codified in 41 CFR part 102-193. Federal agency records management programs must be in compliance with regulations promulgated by both NARA and GSA.

When government agencies establish their own records management program, they can choose to incorporate different requirements. One of the most notable examples is the Department of Defense Standard 5015.2, which dictates how defense agencies must secure and retain classified and non-classified records. This rule, whose directives can be found at http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf, requires records management solutions to be certified before any U.S. Department of Defense agency can implement it.

Because of the transition to information systems, NARA has expanded its mandates to incorporate electronic records—specifically, how electronic records are stored, storage media considerations and facility requirements where these records are ultimately kept (Figure 2). These rules provide some consistency for U.S. federal government records management policies.

FIGURE 2. SELECT SECTION TITLES FROM FEDERAL RECORDS ACT REGARDING ELECTRONIC RECORDS

Regulation	Applicable Section Titles / Descriptions
36 CFR Sec. 1234.1[4]	Scope of Part. This part establishes the basic requirements related to the creation, maintenance, use, and disposition of electronic records. Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic information systems, whether on microcomputers, minicomputers, or

[1] http://assembler.law.cornell.edu/uscode/uscode44/usc_sec_44_00002102----000-.html
[2] http://assembler.law.cornell.edu/uscode/44/usc_sec_44_00003101----000-.html
[3] http://www.archives.gov/about/regulations/part-1220.html
[4] http://www.archives.gov/about/regulations/part-1234.html

	main-frame computers, regardless of storage media, in network or stand-alone configurations. This part also covers creation, maintenance and use, and disposition of Federal records created by individuals using electronic mail applications.
36 CFR Sec. 1234.10[5]	Agency responsibilities. The head of each Federal agency shall ensure that the management of electronic records incorporates the following elements: (a) Assigning responsibility to develop and implement an agencywide program for the management of all records created, received, maintained, used, or stored on electronic media; and notifying the National Archives and Records Administration, Modern Records Programs (NWM), 8601 Adelphi Rd., College Park, MD 20740-6001 and the General Services Administration, Office of Government Policy (MKB), Washington, DC 20505, of the name and title of the person assigned the responsibility. (b) Integrating the management of electronic records with other records and information resources management programs of the agency. (c) Incorporating electronic records management objectives, responsibilities, and authorities in pertinent agency directives and disseminating them throughout the agency as appropriate. (d) Establishing procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. (e) Ensuring that adequate training is provided for users of electronic mail systems on recordkeeping requirements, the distinction between Federal records and nonrecord materials, procedures for designating Federal records, and moving or copying records for inclusion in an agency recordkeeping system; (f) Ensuring that adequate training is provided for users of electronic information systems in the operation, care, and handling of the equipment, software, and media used in the system. (g) Developing and maintaining up-to-date documentation about all electronic information systems that is adequate to: Specify all technical characteristics necessary for reading or processing the records; identify all defined inputs and outputs of the system; define the contents of the files and records; determine restrictions on access and use; understand the purpose(s) and function(s) of the system; describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensure the timely, authorized disposition of the records. (h) Specifying the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements, and maintaining inventories of electronic information systems to facilitate disposition.

[5] http://www.archives.gov/about/regulations/part-1234.html

	(i) Developing and securing NARA approval of records disposition schedules, and ensuring implementation of their provisions. (j) Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically. (k) Establishing procedures to ensure that the requirements of this part are applied to those electronic records that are created or maintained by contractors. (l) Ensuring compliance with applicable Governmentwide policies, procedures, and standards such as those issued by the Office of Management and Budget, the General Accounting Office, the General Services Administration, the National Archives and Records Administration, and the National Institute of Standards and Technology. (m) Reviewing electronic information systems periodically for conformance to established agency procedures, standards, and policies as part of the periodic reviews required by 44 U.S.C. 3506. The review should determine if the records have been properly identified and described, and whether the schedule descriptions and retention periods reflect the current informational content and use. If not, or if substantive changes have been made in the structure, design, codes, purposes, or uses of the system, submit an SF 115, Request for Records Disposition Authority, to NARA.

Local Obligations

In the U.S., while states may have different record retention rules, each have some type of "Sunshine Laws." These laws mandate that certain records—such as real estate documentation, school committee meeting minutes, etc.—are readily available to the public. Some of these records are still paper-based, but more and more of this data is being shared via government websites in order to meet information accessibility requirements. Putting this information onto websites saves local governments agencies some operational headaches (fewer IT staff is need to meet record requests, etc.). The downside is that getting these records management systems and associated storage up and running can put a huge burden on IT staffs, in particular very small ones. However, given the criticality of this information, agencies have little choice: It is imperative that the data they generate is protected and secured.

FIGURE 3. SELECTIVE SECTIONS FROM THE STATE OF GEORGIA OPEN RECORDS LAWS

Section	Applicable Section Titles / Descriptions
§ 50-18-70[6]	Inspection of public records; printing of computerized indexes of county real estate deed records; time for determination of whether requested records are subject to access; electronic access to records. (a) As used in this article, the term "public record" shall mean all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency. "Public record" shall also mean such items received or maintained by a private person or entity on behalf of a public office or agency which are not otherwise subject to protection from disclosure; provided, however, this Code section shall be construed to

[6] http://web.lexis-nexis.com/research/retrieve?_m=316c864163ac278a08ba35e2bd022219&csvc=

	disallow an agency's placing or causing such items to be placed in the hands of a private person or entity for the purpose of avoiding disclosure. Records received or maintained by a private person, firm, corporation, or other private entity in the performance of a service or function for or on behalf of an agency, a public agency, or a public office shall be subject to disclosure to the same extent that such records would be subject to disclosure if received or maintained by such agency, public agency, or public office. As used in this article, the term "agency" or "public agency" or "public office" shall have the same meaning and application as provided for in the definition of the term "agency" in paragraph (1) of subsection (a) of Code Section 50-14-1 and shall additionally include any association, corporation, or other similar organization which: (1) has a membership or ownership body composed primarily of counties, municipal corporations, or school districts of this state or their officers or any combination thereof; and (2) derives a substantial portion of its general operating budget from payments from such political subdivisions…. **(**f) The individual in control of such public record or records shall have a reasonable amount of time to determine whether or not the record or records requested are subject to access under this article and to permit inspection and copying. In no event shall this time exceed three business days. Where responsive records exist but are not available within three business days of the request, a written description of such records, together with a timetable for their inspection and copying, shall be provided within that period; provided, however, that records not subject to inspection under this article need not be made available for inspection and copying or described other than as required by subsection (h) of Code Section 50-18-72, and no records need be made available for inspection or copying if the public officer or agency in control of such records shall have obtained, within that period of three business days, an order based on an exception in this article of a superior court of this state staying or refusing the requested access to such records. (g) At the request of the person, firm, corporation, or other entity requesting such records, records maintained by computer shall be made available where practicable by electronic means, including Internet access, subject to reasonable security restrictions preventing access to nonrequested or nonavailable records

State law can apply to county and city governments and typically include computer-generated records. This requires government organizations to properly prepare storage infrastructures that can retain digital images of real estate deeds, architectural drawings and health care records of state employees.

International Mandates

While the structure of international agencies may be different from those in the U.S. and the laws a lot older, they face similar challenges: More and more information is being created electronically, which means agencies have to adapt their IT infrastructures to meet new storage and availability requirements. For example, there are several acts in the United Kingdom that require government agencies to track agriculture and produce shipments for health reasons. This information must be readily available to prevent epidemics.

The State of New South Wales, Australia, has also extended its record keeping policies and set technology guidelines for electronic records—all to ensure that information is secure and accessible during the required retention period (Figure 4). This includes recommendations for agencies to preserve records and to document

this process as a record in and of itself. From a technology standpoint, this means IT solutions need audit trail capabilities and a means to enforce preservation requirements, regardless of how long the retention period is.

FIGURE 4. NEW SOUTH WALES POLICY ON DIGITAL RECORDS PRESERVATION[7]

Section	Applicable Section Titles / Descriptions
1. Digital State records should be migrated forward as technologies change.	• Records should be routinely monitored in order to identify any formats that are at risk of obsolescence. • Migration of records should be planned, quality controlled and documented. • Public offices should migrate long term value and archival records into stable long term formats so that they do not become obsolete while they are being retained beyond their period of active use. An example of a stable long term format is Open Document Format. • Where records are in unique or legacy formats/systems with no migration paths available, they must be supported by the responsible public office until all retention requirements are met or they are transferred as State archives. Guidance is available from State Records on selecting appropriate preservation techniques for such records.
2. The content and essential characteristics of digital State records must remain unchanged through preservation processes.	• Testing should be used to check that content and essential characteristics of digital records are not compromised by preservation processes. • It is the role of the public office responsible for the records to define records' essential characteristics that must not change as a result of the preservation process.
3. Digital State records must be preserved in context.	• Information needed to understand and use digital records should be linked to or otherwise associated with them throughout preservation processes. • The digital records preservation process itself must be recorded.
4. Digital State records must be secure and tracked throughout the preservation process.	• The preserver should implement security measures to ensure that the records being preserved are not compromised during any preservation process • It must be possible to demonstrate an unbroken chain of custody throughout the preservation process.
5. Digital records preservation programs should be flexible	• Digital State archives will be maintained by State Records in bitstream in addition to any other formats that they are migrated to, in order to take advantage of future developments in digital records preservation. • The preserver should seek to base digital records preservation approaches on non-proprietary technologies to avoid loss of control over Government owned information as a result of changed commercial arrangements in the future.
Definitions	• A "record" means any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means. • "State record" means any record made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public

[7] http://www.records.nsw.gov.au/recordkeeping/

	office, or for the use of a public office, whether before or after the commencement of this section. [8]

The Impact to Storage

Storage Media Requirements

New South Wales is just one example of the worldwide adoption of electronic records management policies for government organizations and agencies. While the regulations are rarely prescriptive, they do say that electronic records have to be stored on some type of electronic media. When making decisions for the type of electronic media they will leverage and the larger IT infrastructure they put in place, government agencies must consider: retention periods, file formats, access and availability requirements and associated IT costs.

NARA too has set forth specific requirements for selecting and storage media for government agencies (Figure 5). While fairly comprehensive, this law does not recommend any type of technology. It does, however, require agencies to back up records and rotate tape media at least every 10 years. This certainly impacts IT environments from a backup perspective, especially as data volumes increase.

FIGURE 5. U.S. FEDERAL RECORDS ACT - ELECTRONIC STORAGE MEDIA

Regulation	Applicable Section Titles / Descriptions
36 CFR Sec. 1234.30[9]	1234.30 Selection and maintenance of electronic records storage media. (a) Agencies shall select appropriate media and systems for storing agency records throughout their life, which meet the following requirements: (1) Permit easy retrieval in a timely fashion; (2) Facilitate distinction between record and nonrecord material; (3) Retain the records in a usable format until their authorized disposition date; and (4) If the media contains permanent records and does not meet the requirements for transferring permanent records to NARA as outlined in 1228.270 of this chapter, permit the migration of the permanent records at the time of transfer to a medium which does meet the requirements. (b) The following factors shall be considered before selecting a storage medium or converting from one medium to another: (1) The authorized life of the records, as determined during the scheduling process; (2) The maintenance necessary to retain the records; (3) The cost of storing and retrieving the records;

[8] http://www.austlii.edu.au/au/legis/nsw/consol_act/sra1998156/s3.html#record
[9] http://www.archives.gov/about/regulations/part-1234.html

	(4) The records density; (5) The access time to retrieve stored records; (6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another (such as from optical disk to magnetic tape); and (7) Whether the medium meets current applicable Federal Information Processing Standards. (c) Agencies should avoid the use of floppy disks for the exclusive long-term storage of permanent or unscheduled electronic records. (d) Agencies shall ensure that all authorized users can identify and retrieve information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling. (e) Agencies shall ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion. (f) Agencies shall back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records shall be maintained in storage areas separate from the location of the records that have been copied. (g) Maintenance of magnetic computer tape. (1) Agencies shall test magnetic computer tapes no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention. This test should verify that the tape is free of permanent errors and in compliance with National Institute of Standards and Technology or industry standards. (2) Agencies shall maintain the storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the following temperatures and relative humidities: Constant temperature -- 62 to 68º F. Constant relative humidity -- 35% to 45% (3) Agencies shall annually read a statistical sample of all reels of magnetic computer tape containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss. In tape libraries with 1800 or fewer reels, a 20% sample or a sample size of 50 reels, whichever is larger, should be read. In tape libraries with more than 1800 reels, a sample of 384 reels should be read. Tapes with 10 or more errors should be replaced and, when possible, lost data shall be restored. All other tapes which might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) shall be read and corrected as appropriate.

	(4) Agencies shall copy permanent or unscheduled data on magnetic tapes before the tapes are 10 years old onto tested and verified new tapes. (5) External labels (or the equivalent automated tape management system) for magnetic tapes used to store permanent or unscheduled electronic records shall provide unique identification for each reel, including the name of the organizational unit responsible for the data, system title, and security classification, if applicable. Additionally, the following information shall be maintained for (but not necessarily attached to) each reel used to store permanent or unscheduled electronic records: file title(s); dates of creation; dates of coverage; the recording density; type of internal labels; volume serial number, if applicable; number of tracks; character code/software dependency; information about block size; and reel sequence number, if the file is part of a multi-reel set. For numeric data files, include record format and logical record length, if applicable; data set name(s) and sequence, if applicable; and number of records for each data set. (6) Agencies shall prohibit smoking and eating in magnetic computer tape storage libraries and test or evaluation areas that contain permanent or unscheduled records. (h) Maintenance of direct access storage media. (1) Agencies shall issue written procedures for the care and handling of direct access storage media which draw upon the recommendations of the manufacturers. (2) External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records shall include the following information: name of the organizational unit responsible for the records, descriptive title of the contents, dates of creation, security classification, if applicable, and identification of the software and hardware used.

Clearly, storage systems play a key role in long-term record retention compliance; however, many government rules do not mention storage systems specifically. This can lead to the misconception that storage does not play a critical role. Record retention regulations are about saving information for long periods of time and storage solutions, although not a primary thought when dealing with some laws, are an integral part of successful records management program.

The Intersection of Information Growth and Compliance

ESG estimates that primary database instances are growing at 25% per year and unstructured data and e-mail is increasing at two to three times that rate. This puts a strain on IT departments—challenging them to find ways to store and protect increasing storage volumes while IT budgets remain flat.

Government agencies are not only dealing with these challenges today, but could be in worse situations than other vertical markets. In the government sector, IT is often an afterthought, particular if budgets are directed to a war or a new educational program. Compliance considerations make an already difficult situation worse. IT now has to deal with electronic records. For example, a state's water resource department has to be mindful of e-mail and electronic records having to do with water levels, water quality, safety inspection of dams, forecasted rainfalls, historical resource contracts, etc.

Storing these records is one challenge, preventing any deletion or modification of the record for the duration of retention periods is another. Further, records must be made accessible to a variety of constituents including military personnel, government employees and ordinary citizens. Even if IT figures out how to store and preserve all these records, they may still have to handle information security rules. For example, the Federal Information Security Management Act (FISMA) details the "laws, policies and directives that govern the creation and implementation of federal information security practices that pertain specifically to grants and contracts."

The Role of E-mail

Despite the rise of instant messaging, social networks and many other forms of collaboration and information sharing, e-mail continues to be a mission-critical tool for businesses and government organizations. E-mail retention, search and retrieval for compliance and legal purposes continue to be major issues for all industries and organizations of every size—and government agencies are no exception. Additionally, as e-mail volumes increase, administrators struggle to meet service-level performance metrics while providing end-users with sufficient access to older e-mail messages.

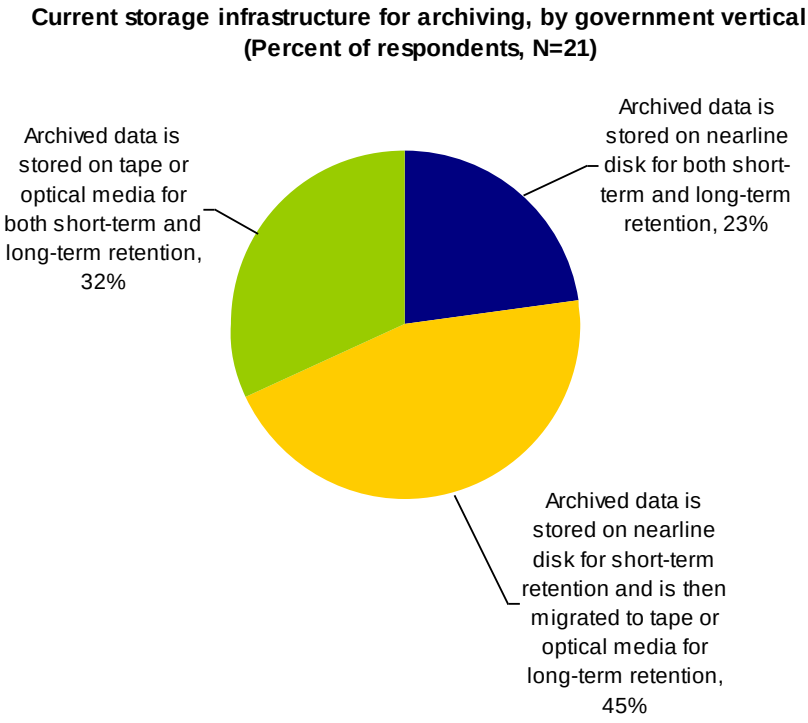
As a result, more and more organizations are implementing some type of defined policy-driven process to govern the retention and protection of older e-mail messages. These range from processes that focus on disaster recovery and backup (i.e., making a temporary copy of a message that is ultimately overwritten) to archiving messages (i.e., physically moving the actually message—not a copy—from one system to another so that a permanent copy of the message is stored without alteration or deletion for a specific period of time).

In the past, many organizations, including government agencies, could meet these requirements with simple backup processes. However, more and more organizations today are finding that operational priorities and regulatory requirements demand a more sophisticated automated, policy-based set of processes and tools that enable not just the long-term retention of messages, but allow organizations to search, index, access and manage e-mails over their life-cycle.

The bottom line is that government organizations relying on traditional backup solutions to retain and produce "requested e-mails" may be forced to rely on manual searches of retained files in order to find the proverbial "needle in a haystack." The good news is that many organizations are implementing technologies and processes to manage the long-term retention of e-mail whether for business, compliance, legal or data/infrastructure management purposes.

Further, ESG research finds that while many organizations are initially storing e-mail and other content on some type of near-line disk platform, 77% have implemented a tiered storage strategy that moves information from disk to tape or optical media after a specified period of time (Figure 6). The reason for taking this type of approach is simple: It allows organizations to balance long-term economic considerations (i.e., system, maintenance and power and cooling costs) with availability and data retrieval considerations.

FIGURE 6. ARCHIVING STORAGE INFRASTRUCTURE WITHIN GOVERNEMENT ORGANIZATIONS / AGENCIES



Source: ESG Research Report: Electronic Discovery Requirements Escalate, 2007

Electronic Discovery Also Applies to Government Agencies

E-mail is the most common source of electronic evidence requested during an electronic discovery. Most associate electronic discovery with the private sector; however, recent activities substantiate that messages are a critical source of evidence for government investigations. For example, there is an ongoing argument in the United States concerning the White House and Office of President deleting e-mail records inappropriately. There has also been discussion of certain White House staff members circumventing formal e-mail systems when discussing political campaign contributions because they did not want the messages to be archived.

Whether you're a large federal agency or a small government organization, electronic discovery is something you must be prepared to deal with. NARA has called out rules for the judicial use of electronic records (Figure 6) E-mails, contracts, employment files, etc are all potential targets. Factor in retention laws that may require organizations to keep data for 30 years or more and organic information growth and it is easy to see how finding a subset of electronic evidence can be difficult.

FIGURE 7. U.S. FEDERAL RECORDS ACT - JUDICIAL USE OF ELECTRONIC RECORDS

Regulation	Applicable Section Titles / Descriptions
36 CFR Sec. 1234.26[10]	1234.26 Judicial use of electronic records. Electronic records may be admitted in evidence to Federal courts for use in court proceedings (Federal Rules of Evidence 803(8)) if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it. Agencies should implement the

[10] http://www.archives.gov/about/regulations/part-1234.html

	following procedures to enhance the legal admissibility of electronic records. (a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach. (b) Substantiate that security procedures prevent unauthorized addition, modification or deletion of a record and ensure system protection against such problems as power interruptions. (c) Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records. (d) Coordinate all of the above with legal counsel and senior IRM and records management staff.

Locating electronic evidence is only one of the challenges that organizations must address. They must also ensure the integrity of data over many years by properly preserving it. This means protecting data against manipulation, modification or deletion over its retention period. Electronic discovery also means that agencies have to find a way to store certain records—potentially those are more likely to be requested—on more accessible storage media.

Archiving for Compliance and Storage Benefits

A New Approach Is Needed

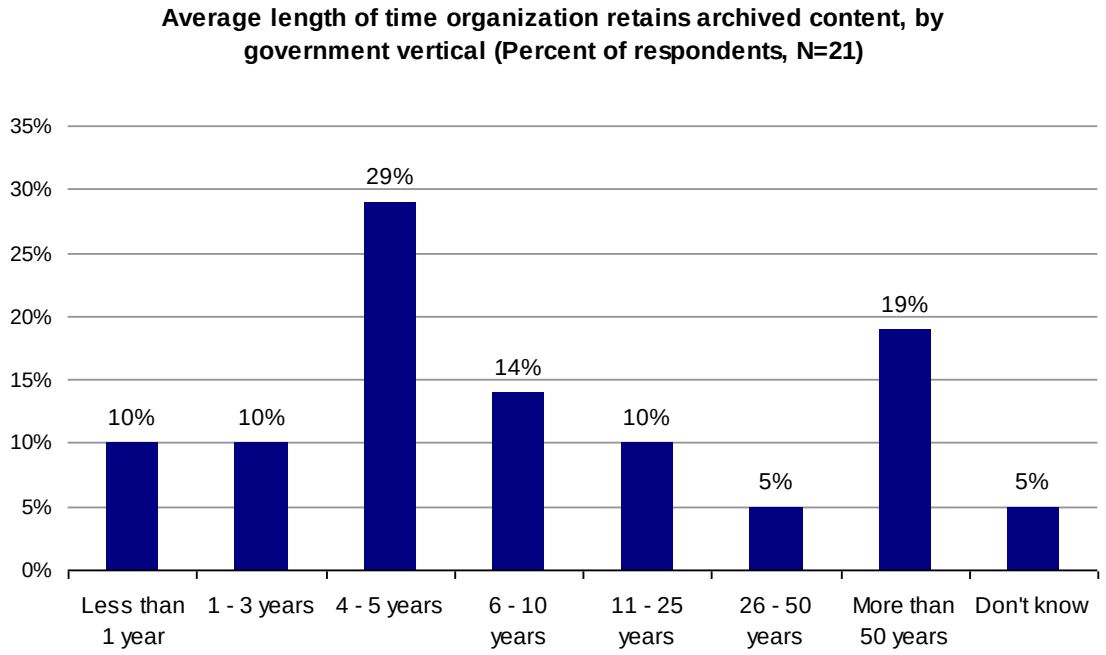
Regulatory compliance, electronic discovery processes and e-mail demands require organizations to think about archiving in an entirely new way. Keeping everything on tape is no longer an option due to varying accessibility requirements due to investigations and Sunshine Laws, but storing everything on disk may be cost-prohibitive despite falling disk prices. The best option may be to incorporate multiple tiers of storage, depending on the type of data and specific regulatory requirements. Data movement and security capabilities must also be considered as agencies look to comply with mandates while improving the efficiency of their overall storage environments.

Organizations should look for archive solutions that adapt to current and future data retention, data authenticity and disaster recovery requirements and are flexible from an application (e.g., e-mail, database, file) and storage (disk, tape, optical) support standpoint. IBM's DR550 allows users to create a flexible data archive—one that allows customers to align technology capabilities with regulatory and IT operation's needs.

IBM DR550 Addresses Key Compliance Challenges

I. **Storing Large Volumes of Data for Long Periods of Time Cost-Effectively**
When combining explosive information growth with longer retention periods, it is easy to see how a government agency's storage budget could quickly get out of control. As an example, an agency may have to keep all legislative meeting videos for 10 years. Other government agencies may need to keep certain data types indefinitely and still others may fall somewhere in-between (Figure 7).

FIGURE 8. AVERAGE LENGTH OF TIME ARCHIVED CONTENT IS RETAINED – GOVERNEMENT



Source: ESG Research Report: 2007 E-mail / Database / File Archiving Surveys, November 2007

The challenge is finding an archive solution that is adaptable—adjusting to specific records management scenarios. IBM offers two DR550 models for government agencies. The 2233 Model DR1 is a single-server, single-rack (25U) system that provides up to 30 TB of usable capacity. It is designed for smaller agencies such as cities or country IT departments. The 2233 Model DR2 is geared to larger government organizations like the British Parliament or the U.S. Department of Homeland Security and scales from 8 TB to 136.5 TB of capacity. Also, the DR2 gives organizations the option to implement two servers for high availability and has synchronous or asynchronous replication options for Disaster Recovery.

The DR550 supports different tiers of media (disk, tape and optical) within the same archive. This can help keep archive costs down (only data that needs to be on disk is kept on disk) and enables agencies to scale archive capacity into the petabyte range should they need to. The migration of the data is automated and policy- or event-driven. Typically, older data or less frequently accessed is migrated data to tape. The movement is handled by the Systems Storage Archive Manager (SSAM). SSAM is a version of IBM's TSM software and is the "brains" of the archived DR550 archive. It runs on an integrated server in the DR550 and defines and enforces retention policies as well as kicks off the data migration process (e.g., moving data from disk to tape or tape to optical).

The SSAM API integrates with more than 40 archiving and content management applications that can feed the system. Some of these applications have been certified by the U.S. Department of Defense to meet the 5015.2 Standard. Defense agencies may choose to manage records with a combination of the certified hardware and software. The retention period is set by the archive application and enforced by the DR550. The system also has a gateway feature, which allows users to bring NFS and CIFS files into the archive and use SSAM to assign retention policies for the data. Data is automatically migrated among the archive media according to policies or specific events.

For government agencies, the level of flexibility in the DR550 is huge. It ensures that data that needs to be readily accessible during a record request (from any party) or investigation inquiry can be kept on disk where data that may be important from, for example, a historical perspective but not have

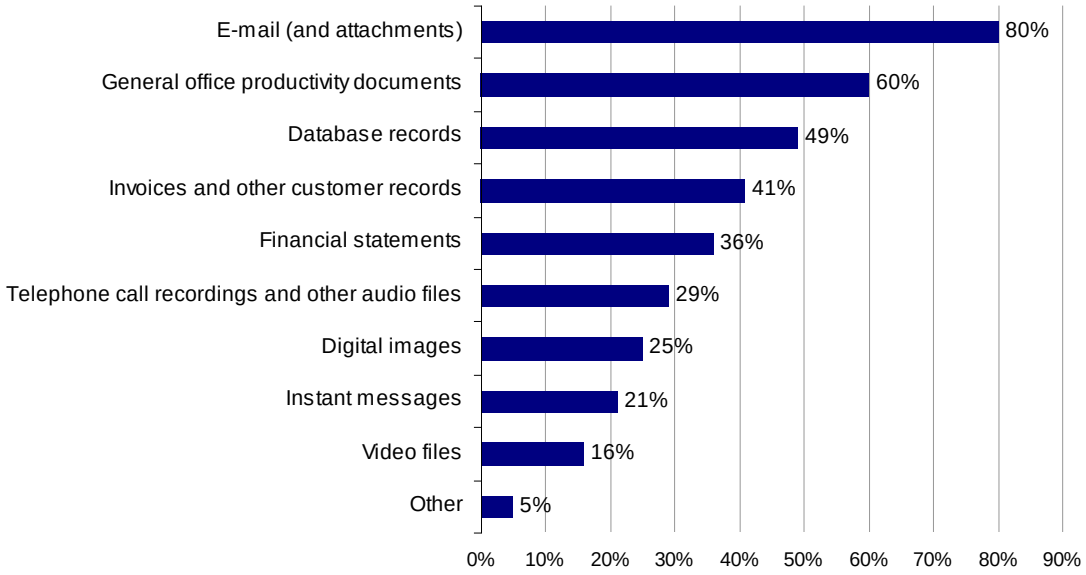
significant access demands, is stored on the most cost-effective medium. For less frequently accessed data, using tape can be more cost-effective over the long term.

II. Centralizing Business Records for Consistent Retention Management

Government records may incorporate e-mail, database data, files generated from imaging, human capital management and other applications. The same holds true for evidence sources as there is no telling what data sources investigators may target (Figure 8). Trying to deploy an archive storage system for each of those applications can create significant IT overhead. IBM's DR550 simplifies this process by creating a central multi-tier archive for all these data types. Data migration is automated and handled by the DR550's SSAM.

FIGURE 9. MOST FREQUENTLY REQUESTED RECORD TYPES DURING AN ELECTRONIC DISCOVERY

To the best of your knowledge, which of the following record types has your organization been asked to produce in a legal proceeding or regulatory inquiry? (Percent of respondents, N = 107, multiple responses accepted)



Source: ESG Research Report: Electronic Discovery Requirements Escalate, 2007

III. Record Preservation and Security

There is a big difference between getting records into an archive and preserving them once they're stored. Being able to do both—and doing it automatically—is critical to government organizations. Given the huge volume of records that these agencies are having to store, it is imperative that the process of preserving critical business records be automated.

The DR550 has an auto-WORM capability, which can be applied to all tiers of the archive (disk, tape and optical). This protects data from being written over or erased. This means records are preserved over their lifetime and, importantly, as data is migrated among the DR550's multiple tiers. Organizations can set retention policies within the DR550 itself or from supported database, e-mail, or archiving applications. Alternatively, the DR550 can be connected to supported WORM-enabled tape libraries.

The DR550 also has support for built-in encryption, which enable organization to encrypt data to secure records that are being transported to an offsite location on tape. The security features can facilitate compliance with rules such as FISMA or HIPAA which is a healthcare industry regulation but many governments operate hospitals for military personnel.

IV. Protecting Corporate Archives

The DR550's integrated media management capabilities have implications beyond archiving. Backups can be initiated directly from the DR550 to tape using SSAM. This is important for a couple of reasons: 1) it makes it easy for users to protect their archives and 2) it is cost-effective because no additional (backup) software is needed. For smaller agencies, not having to buy additional software to protect an archive saves hard to come by budget dollars.

As for business continuity, the DR550 DR2 (enterprise-class) model includes optional synchronous or asynchronous mirroring of archive data for added protection for users' most vital archive data. This data distribution can be helpful to agencies that need to move data between locations such as embassies or consulates. The mirroring is done through onboard software. By replicating data off-site either synchronously or asynchronously, the DR550 helps agencies ensure that critical records are protected in the event of a disaster, thereby fulfilling a critical piece of the business continuity plan.

Conclusion

Complying with information retention and security rules means different things to different government organizations due to the volume and scope of regulations out there. However, the challenge of creating, saving and securing a growing number of electronic records for longer and longer periods is a challenge shared by many organizations today—and government agencies are no exception.

NARA provides an electronic records management baseline for any agency to follow and many have done so. The rules discussing the selection of storage media and handling records with the judicial process in mind reinforce the importance of storage within the compliance process, and New South Wales policies should remind agencies about the transition to the digital records age.

IBM's Information Archiving and Retention strategy allows organizations to optimize their storage infrastructures by matching the value of their information to appropriate storage media (i.e., disk or tape). Doing so gives users the cost benefits of blended solution. While the price delta between disk and tape has narrowed over the last few years, tape is still less expensive to acquire and maintain than disk over the long term and it can offer power and cooling efficiencies over disk.

IBM's DR550 is a unique product in the market that it integrates disk and tape in a single archive, which means it can scale significantly—and, importantly, cost-effectively. Organizations can cost effectively keep data online for extended periods of time and there is no additional operational overhead since software automatically moves data and backs up records according to policies. Because government records often capture the history of a country, state or county, protecting them via replication and securing them with encryption may also be necessary. These capabilities are features of IBM's DR550 solution set.

European countries have been saving government records since the establishment of formal legislatures. NARA was created in 1934 because the U.S. government thought it was essential to preserve vital records. The means of creating and storing these records has changed dramatically but the importance of the information being recorded has not. The role of storage will be increasingly important as government agencies build out infrastructures to meet current and future compliance requirements—eventually becoming part of the compliance process. Which solution is chosen will ultimately determine how efficiently and effectively agencies meet compliance requirements.

20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com