IPRO

WHITEPAPER

Government Survey 2021

Challenging times for data and records management functions at government agencies

For data and records management functions at government agencies, these are some challenging times. Perhaps never before have government entities faced such a high demand for information resources, while at the same time encountering governance, compliance, electronic discovery (eDiscovery), and security requirements that are frequently changing.

Professionals who work in data and records management are seeing demand for all kinds of data, and big data initiatives have become commonplace across many government functions. In addition to rising volumes, data is coming from a growing number of sources and it's taking on more varied forms.

In terms of variety, consider the kinds of data agencies have begun gathering that's outside the realm of "traditional" data that comes in the form of government or legal documents. There's data from Web sites, social media, and the growing number of entities connected via the Internet of Things (IoT) that generate their own set of data.

Many municipal governments have launched "smart city" initiatives in which all kinds of assets are connected in an IoT network and gather data via sensors. These include traffic lights, buildings, vehicles, gas meters, waste management facilities, streetlights, video cameras, and others.

Adding to government data challenges is the fact that not all data is equal when it comes to security, privacy, compliance, and governance. Some information is far more sensitive and proprietary than others. Sorting out the various types of data and the security and compliance needs for each and making the data accessible to those users who need it is often difficult. That's especially true when the data is stored in silos within different departments or groups.

Also adding to the complexity of data and records management are the ongoing moves to the cloud and continuing work-from-home trends that began in 2020 as a result of the COVID-19 pandemic. Many agencies are moving more and more workloads to the cloud, creating hybrid IT environments.

As if all this wasn't enough, agencies are having to fulfill a growing number of Freedom of Information Act (FOIA) requests on a regular basis.

Finally, agencies—like so many private businesses—are in the midst of digital transformations that are changing the way many processes are handled. Many services, such as acquiring necessary permits, are now digital. And this results in even more electronic data to manage.

To get a clear sense of what government organizations are doing to address the myriad challenges they face and take advantage of the opportunities presented to them, IPRO in the first quarter of 2021 conducted an online survey of records management, legal, IT, data privacy, risk and compliance, information security, and executive/management professionals in government.

The respondents represented all levels of the government, including federal, state, county, and city agencies around the U.S. They weighed in on topics including the top FOIA challenges they're facing this year; which facets of information governance are most important to their agency; and which new technologies they are most interested in adopting.

FOIA Challenges

Respondents were asked to identify the top challenges they expect their agencies to face this year related to FOIA. At the head of the list was reviewing records, cited by 36% of the professionals. This could be due in part to the sheer volume of FOIA requests.

36% REPORTED REVIEWING RECORDS **TOP FOIA CHALLENGE**

In a March 2021 report, the U.S. Government Accountability Office (GAO) said federal agencies reported that they processed nearly 878,000 FOIA requests for government information in 2019, an increase of 32% since 2012. Another GAO report found that the backlog of FOIA requests had grown more than 80% since fiscal year 2012, driven in part by increased requests.

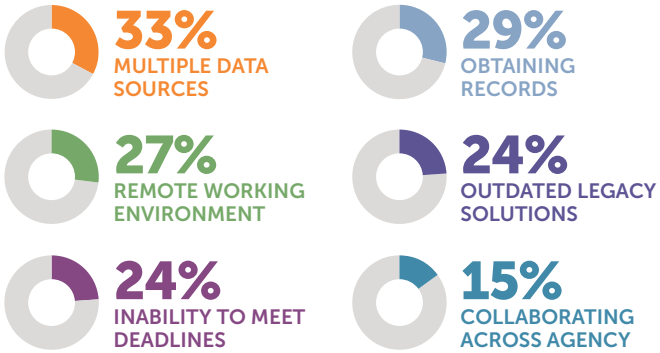
"The volume of electronic records being created by electronic devices—iPhones, laptops, etc.—is challenging on several fronts," says Jay Olin, director of Division C of FOIA analysis at the Centers for Medicare & Medicaid Services, part of the Department of Health and Human Services.

"First, the sheer volume of pages when combining e-mail and their attachments will turn a FOIA request into thousands of pages," Olin says. "Converting e-mail into Adobe to perform a FOIA analysis with redactions may take hours or days, depending on the software used for the task. And conducting a line-by-line review and removing duplicate records might take months of laborious and tedious work by the FOIA analyst.

Also scoring high on the list of FOIA challenges was dealing with multiple data sources, mentioned by 33% of the respondents.

"Calendar records of agency officials is one source of records that require extensive review and redaction for personally identifiable information [PII]," Olin says. "Requests for data in a particular database may require a contractor managing the database to spend multiple hours creating a 'public use file' stripped of PII and/or protected health information.

Other common responses included obtaining records (29%), remote working environment (27%), aging infrastructure/outdated legacy solutions (24%), inability to meet deadlines (24%), and collaborating across the agency (15%).



What's particularly interesting is the variety of challenges many professionals are facing with FOIA. Some of these involve technology, others have to do with processes, and still others are related to the new workplace arrangements. It's important for agencies to note that many of these hurdles can be addressed through effective records management and the use of data management offerings such as data governance platforms.

"Proper records management is a crucial part of the FOIA process," Olin says. "Providing access to the records will result in timely responses to the FOIA office processing FOIA requests."

Information Governance

A strong information governance strategy is vital for government agencies, for the simple reason that data is a precious resource in the digital economy, and protecting the security, privacy, and integrity of it should be a major priority. A lot of data contains personal information, and it's at constant risk from breaches, malware, and other cyber threats.

Agencies often store data or move it back and forth among on-site and off-premises data centers, private and public cloud services, mobile and edge devices, and the IoT. That broad ecosystem makes securing data much more challenging. In addition to security, agencies need to be cognizant of requirements related to privacy regulations, the need for timely and accurate data, and other issues.

All of this relates back to information governance. Without it, agencies face the possible chaos with records and data management. GAO has noted that effective data governance is a key component to ensure data quality.

The IPRO survey asked professionals which facets of information governance will be important to their agency in the coming years. The most common responses was records and information management, cited by about two thirds of the respondents. This is not surprising

because it encompasses all that these professionals are striving to achieve with governance.

The next most often cited facet of governance was information security and protection, mentioned by 48%. Agencies are under attack from a large array of threat vectors, including hackers and other cyber criminals, state-sponsored attackers, malware creators, hacktivists, and others. These bad actors are using increasingly sophisticated methods to get to valuable data.

"It is an extremely real threat, and most people don't want to think about it," says Meryle Tank, a paralegal in the Office of the City Attorney of San Francisco. "People think they are protected because IT deals with security. The people who I meet who take it seriously have usually themselves experienced a data security breach."

Aging systems that control key resources are far more vulnerable than people realize, Tank says, "as hackers have the newest tools and techniques that can wreak havoc on the unprepared."

Another important facet of governance is compliance, cited by 40% of the respondents. This of course should be no surprise, given the growing number of regulations dealing with data privacy.

"I don't think the average worker realizes how much it is their responsibility to be vigilant about data security, and instead sees it as a burden to getting their work done," Tank says.

Rounding out the list of information governance priorities were data storage and archiving (40%), privacy (37%), data governance (34%), eDiscovery (30%), knowledge management (25%), risk management (21%), and audit (13%).

Outsourcing Trends

Outsourcing in general is on the rise, as organizations look to bring in help from outside the organization to deal with specific skill shortages or general resource limitations, to complete projects more quickly, or for some other reason.

An April 2021 report by Research and Markets noted that the workplace services market was valued at $88 billion in 2020 and is projected to reach $193.4 billion by 2028. It's expected to expand at a compound annual growth rate of 11% from 2021 to 2028. The services comprise end-user outsourcing and technology support services, the study said.

So it's somewhat surprising that a majority of the IPRO survey respondents (72%) said they do not expect their agency to outsource any professional services in 2021.

Of those agencies that are outsourcing IT, legal, and other processes, the most common reason cited for doing so was a lack of internal resources (43%). Other reasons include to improve productivity (26%), aging infrastructure and outdated legacy solutions (20%), lack of internal end-user training (10%), inability to meet deadlines (10%), and to reduce risk (7%).

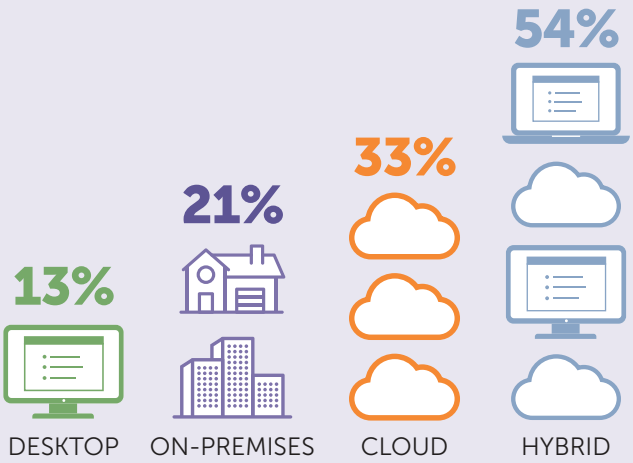
Shift to the Cloud

A large majority of the survey respondents (78%) said their agencies are moving toward greater cloud usage and storage in 2021 and beyond. That reflects a general shift to the cloud that began several years ago and accelerated in 2020 in part because of the remote work trend.

"COVID demonstrated the need for telework abilities that include processing and releasing large files of records," Olin says. "Before [the pandemic], my agency would burn records onto a CD-ROM for release to a FOIA requester if the files were too large for e-mail. Now, with a cloud system such as Box, we are able to upload the files, grant access to the requester, and allow them to download them at their convenience."

When adopting new technologies, more than half of the respondents (54%) said their agency is primarily interested in a hybrid of desktop and cloud technology. About one third said they are primarily interested in cloud technology, 21% are focused on on-premises technology, and 13% are most interested in desktop technology.

Government Agencies are now interested in:



These findings reflect what's going on in both the government and private sector--a trend toward a hybrid IT environment. Organizations want to have a mix of cloud services and on-premises IT, which can provide a high degree of flexibility and agility.

A growing number of agencies are using the cloud for applications, software development, and even to provide their IT infrastructure. The cloud offers ways to reduce capital expenses and increase agility. And at a time when data storage needs continue to grow at a rapid rate, the cloud offers virtually unlimited capacity.

Some government IT strategists are still concerned about whether the cloud is secure enough, or whether they will lose some control, Tank says. "However, time has shown us that our most important data is already in the cloud, and can be secured with proper handling," she says.

Government agencies that are slow to embrace change such as cloud adoption "have been forced to concede that these

systems are powerful and will be a slice of the data pie whether they embrace the concept or not," Tank says.

When selecting cloud service providers, one of the biggest determining factors is whether the provider has been approved by Federal Risk and Authorization Management Program (FedRAMP), a program established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government.

FedRAMP says it empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information. When adopting new technologies, nearly two thirds of the survey respondents (62%) said having a cloud service option with a FedRAMP-approved cloud service provider is important to their agencies.

"FedRAMP appears to meet the requirements agencies seek: A cost-effective solution to allow the sharing of data while protecting the data and records," Olin says.

Conclusion—A Challenge Agencies Must Meet

Data and records management has quickly become one of the most vital functions within agencies at all levels of government. Government is involved in seemingly every aspect of cititzens' lives, and the data and records they gather help them support their missions to serve the public in countless ways. Without the smooth flow of data, many processes would simply come to a standstill.

As a growing number of smart city initiatives emerge, local agencies will be taking in and managing ever-growing amounts of data. These are complex efforts that leverage technologies such as the cloud, edge computing, data analytics, artificial intelligence, IoT, collaboration tools, mobile devices and apps, and others—each churning out enormous volumes of data.

Developing a strategy to manage data while at the same time addressing needs such as governance, compliance, eDiscovery, cyber security, and increasing requests for information by the public will be a daunting challenge. But it's one that agencies must meet in order to achieve their missions in the digital age.