



# How to Find and Process Data With a Data Risk-Management Platform

**MARKET TRENDS REPORT**



**exterro**<sup>®</sup>

# Introduction

---

Government agencies face intense pressure when it comes to accessing and using data. They need it to drive mission outcomes and for legal and regulatory reasons. But the sheer volume of information makes data management challenging, and inadequate processes expose agencies to a range of possible hazards.

“When they don’t fully understand what they have, it opens them up to a number of risks,” said Adam Johnson, Regional Vice President for Public Sector at Exterro, whose solutions help organizations gain deep insight into data across a complex enterprise infrastructure and manage that data more effectively.

One area that makes this problem apparent is in the government’s fulfillment of Freedom of Information Act (FOIA) requests. When data is fragmented and uncontrolled, agencies risk missing the mandatory timelines for responding to those inquiries. They also become vulnerable to legal and regulatory liabilities.

Some agencies will try to fix the problem by keeping too much data, for too long. “Government organizations may have a requirement to hold a certain piece of data for, say, seven years, but instead they’ve held 15 years’ worth of data,” Johnson said.

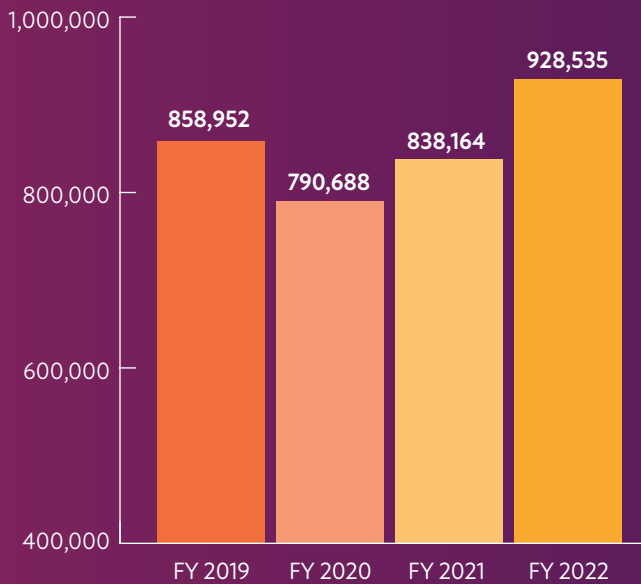
That only exacerbates the issue, however. “They might not want to have to share all of that, but under certain regulations, if they’ve retained it, they have to,” he said. There’s potential legal liability, and of course there’s just that much more data to manage.

To minimize risk, and meet their statutory obligations effectively, agencies need a new approach. They need a data risk-management platform, a system that elevates their capabilities around discovery, privacy, data governance, digital forensics and cybersecurity compliance.

# By the Numbers

In FY 2022, 120 federal agencies were subject to the FOIA. The federal government overall received a record high total of 928,353 FOIA requests, about an 11% increase from FY 2021.

## Total Number of Requests Received



# 333%

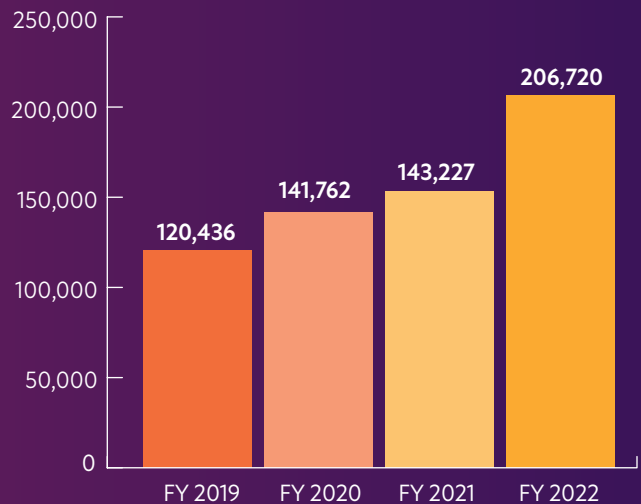
was the increase in the file sizes of public-sector FOIA responses during the pandemic.

***Of the \$584.8 million government spent fulfilling FOIA requests in fiscal 2022, the most recent reporting year, “nearly 93%...of total costs were attributed to the administrative processing of requests and appeals by agencies.”***

– [Department of Justice](#)

The total number of backlogged requests across the government at the end of FY 2022 was 206,720, a 34.9% increase from the number of backlogged requests reported at the end of FY 2021.

## Number of Backlogged Requests



# 149 zettabytes

is the amount of global data expected to be generated in 2024. To handle all that data in the public sector, government cloud spending is forecast to surpass **\$41 billion** in 2024.

# 120

business days is how long agencies have to respond to a FOIA request.

# Addressing Risk in Data Management

---

## Challenges Surrounding Government Data

Several hurdles impede the government's ability to meet its regulatory and legal obligations around the effective use of data.

**Too much data:** Government generates an avalanche of data each year, and agencies' tendency to retain more than is necessary only amplifies the volume they must manage. With too much data on hand, government bares itself to risk.

"There's often not a full understanding of what type of data they have retained, including personally identifiable information or even certain types of classified or unclassified data that is residing in areas that it shouldn't be in," Johnson said.

**Poor collaboration/data sharing:** FOIA and public records requests require agencies to share data internally, yet different businesses units often don't have access to one another's data.

"Identifying the data that's being requested, knowing who's doing what throughout that process: That should be a collaborative effort," he said. Existing systems often don't support that level of cooperation.

**Manual processes:** Too often, agencies fulfill FOIA requests manually. "In some cases, people are just tracking requests in a spreadsheet, trying to keep that up to date as to what's been done or who it has been assigned to," Johnson said.

In many cases, they track everything manually throughout the data discovery life cycle. That's not just the surfacing of data, but the review process and the necessary redactions that are typical of a public records request.

**Pressure to improve data discovery:** Under the Pentagon's Cybersecurity Maturity Model Certification (CMMC) program and other guidelines, agencies must be more effective in their data discovery efforts.

"There's a need to identify unclassified information that's tagged appropriately as unclassified, and to ensure it's in the proper locations. That involves scanning petabytes of data," Johnson said.

## Solution: A Modernized Approach

A data risk-management platform can help agencies increase safety and meet their obligations. Such a solution creates a unified process around data, empowering teams to optimize e-discovery, privacy and data governance, digital forensics, and cybersecurity compliance operations. Key features include:

**Enhanced discovery and e-discovery:** The platform captures metadata, a significant capability when it comes to organizing data stores. "Metadata tells us what type of data this is without actually collecting it," Johnson said. Business units can use the data without adding to the existing weight of unnecessary data holdings.

Electronic discovery, or e-discovery, is the ability to collect and interact with data effectively. "An e-discovery capability is focused around litigation," ensuring agencies can use and preserve data in a way that's legal, defensible and explainable, Johnson said.

**Artificial intelligence (AI):** A modern data risk-management platform will leverage AI to help the organization better understand how users interact with the system. "It can look at what kind of tags they're applying to certain types of data, for example, and make recommendations," Johnson said.

Advanced AI can also define routine tasks, "and it can be used to automate those tasks, as opposed to clicking all those buttons to achieve whatever outcome is needed," Johnson said.

**Early Case Assessment:** This capability enables agencies to understand what data is available before collecting that data. It comes into play even before the metadata tagging goes into effect.

"With early case assessment, you're reaching out to the native data source to see what's there," Johnson said. "You can interact with the data without actually collecting it or bringing it into the platform, without duplicating that data."

# Best Practices

---

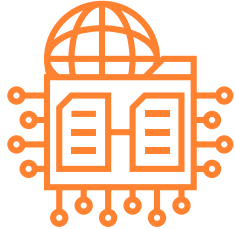
*Best practices can help federal agencies get the most value out of a data risk-management platform.*



## **Create cross-functional teams**

The need to surface relevant data “spans many groups, whether it be it a legal team, a forensics team [or] privacy-focused teams,” Johnson said.

A modernized platform “will support that vital cross-functional capability,” he explained. “For those mature organizations that really do want to embrace the full benefit of a system like this, they can make the tools available across all those different teams and get them all on the same page to create a unified process.”



## **Conduct a comprehensive data audit**

To make full use of the platform, it’s helpful to first build an inventory of the data on hand. “When it comes to fulfilling a public records request or a litigation request, if you don’t know what you even have or where it is or who has access to it, you’re creating a lot more work and more risk,” Johnson said.

By starting with a solid inventory, “you can use the platform to start interacting with the data much more quickly and effectively,” he said. With a reliable inventory, “when you have those requests where you have to collect data, review data, share data, you know exactly where to go and what you have.”



## **Assess legal and regulatory requirements for data retention**

Without a full understanding of the legal and regulatory necessities, “you really don’t know what you even need to keep and for how long,” Johnson said. “If you’re not aware of what those requirements are, then you most certainly will either over-collect or delete data before you should.”

The platform can support any number of processes, but the organization needs to know what’s required in order to define those processes appropriately.



## **Train employees and break down organizational silos**

Agencies need a collaborative environment to drive effective data discovery, and they need to train their employees on the platform to maximize the benefits of that collaborative approach.

“Teams should be trained properly on how to use this platform, and leadership should keep things fresh with training portals and other resources,” Johnson said. “Users should also have an understanding of the best ways in which similar agencies or organizations are utilizing the platform to support their complex processes.”



## Use Cases

---

The federal government faces a range of pressures around data availability, such as compliance requirements and potential legal liabilities tied to managing data poorly. A platform approach can help agencies address several urgent use cases around data discovery and management.

- **Data Risk Management:** Agencies create legal risk when they don't know what data they have or where it resides. Weak data-management practices further open the agency to cybersecurity risk, the reputational risk associated with bad press, and fiduciary risks in the form of fines for noncompliance. Robust data discovery capabilities can minimize those threats.
- **Discovery and E-Discovery:** To meet regulatory and legal goals, agencies need a strong data discovery capability. The ability to meet FOIA requests depends on knowing what you have and where to find it. With metadata classification, a platform approach makes this possible while also minimizing risk by avoiding the ingestion of extraneous or unnecessary data. With an eye toward evading litigation, agencies can use e-discovery to interact with and preserve data effectively.
- **FOIA Activities:** Under FOIA, agencies have mandatory timelines for delivering on public information requests, and many routinely fall short. Strong behind-the-scenes processes, including data-sharing mechanisms, documented workflows and automated reporting capabilities, empower agencies to better manage their FOIA responses.
- **Privacy Regulations:** With more states enacting privacy regulations that give residents the rights to access, correct or even delete PII, government agencies need technology and processes to search the data they hold, identify data associated with an individual and take appropriate actions. To do so, they must understand what PII they hold, where it is, why it is being retained and how long they may retain it.

## HOW EXTERRO HELPS

Exterro's data risk-management platform can help the government better meet its obligations. "It creates a cohesive, unified process to bring different parties together, allowing users to interact with data in a manner that is safe and defensible," Johnson said.

With a platform solution, "you get the ability to truly understand what data you have, where it is, who has access and what they are doing with it," he said. In addition, the risk-management platform supports the reporting needed to validate that agencies are meeting their regulatory requirements and to minimize legal risk around data use.

"We enable them to meet their obligations, and to do so in an efficient manner — to do more with less," Johnson said. "Every agency is challenged in terms of resources, and yet data is growing exponentially. A tool like Exterro helps them to meet their objectives, while minimizing risk across the data life cycle."

*Find out more about how Exterro supports government agencies to manage data risk at [exterro.com/public-sector](https://exterro.com/public-sector).*

# Conclusion

---

With the volume of data ever increasing, government is under pressure to manage that data more effectively, both to meet its public records requirements and to mitigate against cyber, legal and noncompliance risks.

Out-of-date processes make it difficult to manage data appropriately, especially given how much data exists in government agencies. Siloed holdings and an inability to share data further compound the legal and regulatory threats. Indeed, fragmented and uncontrolled data creates a range of compliance issues and potential liabilities.

Agencies can look to a data risk-management platform to unify processes across the data life cycle, helping them better understand what data they have, where it resides and how best to access it when needed for public information or legal inquiries. All of this helps agencies improve their processes around discovery, privacy, data governance, digital forensics and cybersecurity compliance.

## ABOUT

---



Exterro provides busy legal and IT leaders powerful technology solutions to navigate complex data risks successfully. Built on the industry's only data risk management platform, our software suite gives organizations the power to manage e-discovery, privacy compliance, data governance, digital forensic investigations, and cybersecurity response operations in a unified platform. Our software is used by thousands of industry-leading businesses, government agencies, and law firms across the world.

To learn more about Exterro and our data risk management solutions, visit [exterro.com](http://exterro.com).



GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).



1152 15th St. NW Suite 800  
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

[www.govloop.com](http://www.govloop.com)  
@GovLoop

