The data governance and compliance challenges facing state and local governments

By Ryan Schradin
Managing Editor at
GovDataDownload

There are three converging trends that are making the management of data increasingly difficult but incredibly important for today's state and local government agencies. Their modernization, IoT, and other digitization programs are generating mountains of data unlike any that they've needed to store and analyze in the past. Their networks have become increasingly complex thanks to the evolution of modern multi-cloud environments. And, they need to meet and abide by the data privacy requirements prescribed by recent laws like the E.U.'s General Data Protection Regulation (GDPR), as well as longstanding laws like the U.S. Health Insurance Portability and Accountability Act (HIPPA).

Together, these three trends have made data governance more important than ever before – but have also made compliance more difficult, as well.

How have state and local agencies been faring with these higher data volume rates? How have they adapted their data governance processes to ensure the utmost security of the sensitive data they house? And how are they able to achieve and maintain compliance with the growing number of data privacy laws that are being enacted upon them?

To answer these questions, and to learn more about the available solutions that can ease SLED agencies' data governance growing pains, we sat down with NetApp CTO Jim Cosby.

GovDataDownload (GDD): Can you define data governance for our readers who might not be familiar with the concept? What is data governance, and why do organizations need it?

Jim Cosby
NetApp CTO

Jim Cosby: Data governance can have many definitions, depending on the agency or organization. Essentially, data governance is a set of steps and processes on how to manage an organization's data assets, which will help set forth the rules and authorities around how to manage the data for that agency or company. This can include the privacy, integrity, and security aspects of the information, as well. Some institutions will require that data be securely handled if it is considered sensitive, like how medical patient data is covered under HIPAA regulations.

Another example is PII (Personally Identifiable Information) which – like personal financial data and credit card information – is often required to be securely handled per PII protection guidelines. There are many aspects of data governance depending on the federal agency, which can include data stewardship, data quality, data standards, policies, regulatory compliance, privacy and ethics, and many more.

GDD: Let's focus specifically on state, local, and municipal government organizations – what kinds of data do these organizations aggregate, store, and manage?

"Most agencies have good intentions of meeting the data governance rules and compliance requirements, but because of all the changes and limited resources, they sometimes don't know what they have or what they need to do. As a result, they fall out of compliance."

Jim Cosby

Jim Cosby: State and local government data can include any data used for the purpose of their agency mission and business. This can include any business information, documents, media, records, legal information, census data, social data, achievement data, program data, demographic data, and many more.

In some instances, this data can be incredibly sensitive – and incredibly valuable to malicious actors. For example, some colleges and uni-

versities may store sensitive healthcare data about their students if they have a health services center. And state and local government agencies will certainly store the PII of constituents that are enrolled in government programs or applying for government services. The sheer amount of this data has only exploded since the beginning of the pandemic, when agencies were forced to move many of their processes and applications online

GDD: Why is it important that there are policies, procedures, and processes in place dictating how this data is stored, where it can be stored, etc? How can proper data governance help agencies operate better? How can it help keep constituents safe?

Jim Cosby: Though some of it is public, much of this data is considered sensitive and private. This will determine the appropriate management practices around the data.

Some data is essential to public safety, like local government and police data that are used to govern and protect our cities, communities, and citizens. This data requires extra care in handling and management than the public data that may be available to everyone, like public parks and recreation data.

GDD: It's one thing to establish policies and processes for aggregating and storing data, it's another to follow them. Why would government agencies struggle with compliance? What challenges do they face? And do we often see state, local, and municipal government organizations fall out of compliance?

Jim Cosby: Government agencies are all facing multiple challenges these days, like budget cuts, reduced IT staff, an increase in security threats, and ever-changing governance and compliance rules. These are all amplified by current supply chain impacts, making it even harder to know what each agency has – or what they need – to protect. And don't forget about the impact of the mandates and regulations that are currently in place.

Most agencies have good intentions of meeting the data governance rules and compliance requirements, but because of all the changes and limited resources, they sometimes don't know what they have or what they need to do. As a result, they fall out of compliance.

GDD: How has the introduction of the cloud impacted data governance? Has the cloud injected any additional complexity into the process?

Jim Cosby: Cloud adoption has compounded the tasks around data governance and compliance because data is now beginning to extend across multiple clouds, locations, and network perimeters. This digital transformation has unintentionally exposed data to many more touch and management points, as well as to many more users and data administrators.

These new vulnerabilities emphasize the importance of knowing and following data governance and compliance to ensure the data and information are well protected.

GDD: What tools and solutions are available to help these organizations stay compliant with data governance?

Jim Cosby: The first step in data security is understanding what data you have and what requirements are around the different data types. This is best achieved by taking an inventory of all the data an agency houses. NetApp has a Cloud Data Sense service that can run in the cloud and on-premises to analyze any agency's data as well as categorize the data into risk categories including things like PII, HIPAA, GDPR, CCPA, and others. You can also specify specific data types and attributes for Cloud Data Sense to use in searching an agency's data. The interface includes a dashboard that shows what data an agency has, what types of data they have, and what they need to protect and manage in order to be secure and compliant.

Since it became available to the public in late November of last year, more than 100 million users have raced to test out the capability and functionality of ChatGPT. They've asked it to plan out the perfect vacation to the nation's capital. They've asked it to tell them jokes and funny stories. They've even tried to leverage the tool to get out of work – with mixed results.

Many that have read these stories about the ChatGPT artificial intelligence (AI) chatbot might think of it as a novelty – a fun toy to play with around a table with some friends or a neat tool that can explain difficult topics. But others see the potential that this AI technology has for changing the way large organizations and enterprises handle everyday tasks and functions.

Someone with a real vision for how AI solutions like ChatGPT could revolutionize the government is Jon Stresing, an account manager at NVIDIA who works with the U.S. Department of Defense (DoD). We recently had the opportunity to sit down with Jon to discuss the ways in which NVIDIA is opening the door to the wide adoption of AI tools and solutions in the federal government.

During our discussion, Jon explained some of the use cases that he envisions for AI solutions in the government, and why he thinks that AI will change the way the government functions in the not-too-distant future.the government is Jon Stresing, an account manager at NVIDIA who works with the U.S. Department of Defense (DoD). We recently had the opportunity to sit down with Jon to discuss the ways in which NVIDIA is opening the door to the wide adoption of AI tools and solutions in the federal government.

During our discussion, Jon explained some of the use cases that he envisions for AI solutions in the government, and why he thinks that AI will change the way the government functions in the not-too-distant future