In the federal government, perhaps more than any other entity in the country, data is growing at an unprecedented rate. And that includes not only documents but images, video, audio, sensor data, email, social media files, and more. Without structure, data becomes virtually impossible to find when it’s required for eDiscovery, Freedom of Information Act (FOIA) requests, and compliance with retention mandates. It also becomes much more difficult to apply the type of sophisticated analytics necessary to unlock the true value of that data. Finally, lack of structure also makes it difficult to ensure that data is fully secure in compliance with federal regulations.

The solution to these issues is information governance. Gartner defines information governance as an accountability framework that regulates the valuation, creation, storage, use, archival, and deletion of information. It includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in helping an organization achieve its goals.

We spoke with two experts about how agencies and departments can best coordinate efforts and employ the right technology and methods to meet federal mandates while reducing risk and lowering costs. Tom Kennedy, director of Symantec’s Public Sector Emerging Solutions Team, has focused on federal technology for most of his career. He is an active member of the Industry Advisory Council, as well as a member of several organizations focused on bringing government and industry IT leaders together. Matt Nelson, senior eDiscovery and information governance attorney at Symantec, is a leading authority on how technology can help reduce legal risk and cost.

**When people talk about information governance, what exactly are they referring to?**

**Nelson:** Information governance is one of those terms that mean different things to different people. In a lot of ways, it’s similar to what used to be called information lifecycle management. Both of these terms are umbrella concepts that encompass a lot of different objectives. They include protecting critical information, managing data growth, and making sure you have the right tools to discover information when faced with things like eDiscovery, investigations, and FOIA requests. In a nutshell, information governance is about protecting, managing, and discovering information, and doing so in a consistent way. It is a comprehensive approach that involves people, policy, and technology.

**Is information governance more critical to federal agencies than to private enterprises?**

**Kennedy:** It’s important to all entities, but government agencies are held to a higher standard. For example, all agency communication – which today includes not only documents but emails, texts, and tweets – is required to be documented and preserved based on the Federal Records Act. That requires knowing where information is, what’s important, and how to access it.
There have also been many directives in recent years that emphasize the need for information governance. One of the most important is the Presidential Directive on Managing Government Records, which came out in 2011. To support that directive, the Office of Management and Budget and the National Archives have teamed up to release a series of guidance documents on what agencies need to do to comply. The crux of it is that agencies need to digitize their records, and they have to digitize all records – not just current records but past records – by 2019. In September, the government put out additional guidance around managing email that strongly discouraged the print-and-file approach.

How can an agency benefit from beginning a true information governance program?

Kennedy: At the most basic level, an information governance program is the best way to ensure that agencies comply with the directives and mandates that require records management and retention. It also helps agencies more easily respond to Congressional queries quickly and defensibly, and reduces eDiscovery risk. But that’s only the first layer. By employing a comprehensive strategy, agencies are essentially moving from a reactive to a proactive strategy. That allows them to respond to FOIA requests in a more timely fashion, which has been a pain point for many agencies. It allows agencies to be ready, at any point in time, to produce information required by litigators. It also provides the structure and tools to be able to defensively delete documents in a confident way, knowing that all of the rules are being followed and everything is fully secure.

Nelson: One thing that often gets lost in all of this is the cost savings that an information governance strategy can produce. A recent Gartner report estimated that it cost $5 million per year to store and manage just one petabyte of information. A large government agency might have 10 petabytes of information. That’s $50 million to manage and maintain the data. There has also been research from the Compliance, Governance, and Oversight Council showing that 69% of the overall enterprise data has no legal, business, or regulatory value. That means that more than $34 million of federal money probably doesn’t need to be spent, because the data doesn’t need to be retained.

While information governance involves people and policy, it also requires technology. What types of technologies are most important?

Nelson: Endpoint and network security tools are critical to securing the core network and all connected endpoints from intruders. From an IG perspective, establishing a secure network perimeter prevents unauthorized users from gaining access to a network and stealing information such as IP, personally identifiable information (PII), or trade secrets, or actually causing physical damage to critical infrastructure systems.

Data loss prevention and encryption technologies allow organizations to protect sensitive data from unauthorized access and prevent confidential data from leaving a defined information security safe zone such as within an internal agency network. DLP tools can identify information such as Social Security numbers, names, addresses, and other types of PII before they actually leave a protected network. For example, if a user accidentally sends an email with a spreadsheet containing a data dump full of the agency’s HR information, DLP tools could block the transmission of this sensitive information outside of the organization. These technologies have the ability to manage confidential data wherever it is stored and used, across endpoints, mobile devices, networks, and storage systems.

Other important technologies include mobile
device management to protect sensitive data and applications and reduce the risks involved with remote connectivity, and information intelligence technologies such as advanced analytics and visualization tools. These tools help agencies understand what data exists, how it is being used, how often it is used, who owns it, and who has access to it.

Backup and disaster recovery technologies enable organizations to maintain current systems in the event of a catastrophe or serious system failure, while archiving technologies allow agencies to consolidate multiple data sources and types into one centralized repository. Finally, eDiscovery tools, which incorporate advanced data analytics and search capabilities, can help organizations reduce risk in the discovery process and eliminate nonresponsive and irrelevant data.

Who should lead the information governance effort in federal agencies?

**Kennedy:** Information governance spans functions. It includes IT, legal, records retention, security, investigators, and FOIA professionals. Most organizations today still operate in a more siloed fashion, where the records-management people focus on making sure the agency is complying with records-management requests, the legal team focuses on eDiscovery, and so on. But that approach can lead to overlap and other issues.

We’re starting to see a few federal agencies create a new position called Chief Data Officer. This position is designed to manage all of these different interests from different stakeholders so they can have a more coordinated information governance plan. It makes sense, because it’s a root-cause problem that needs to be solved in a coordinated fashion. The idea is growing in private industry and more slowly in federal government, but I think we’ll see it start to take off as more agencies realize the benefits of an approach like that.

**What are some of the struggles facing federal agencies when it comes to building and implementing an effective information governance program?**

**Nelson:** Part of it is a cultural issue. Lawyers who spend their careers dealing with litigation and eDiscovery want to focus on those parts of the process. Somebody who has been a lifelong records manager will be more concerned with complying with federal record-keeping requirements and how to reduce the amount of information the organization is keeping. Then there are people on the security and IT side, and they will see the challenges differently. It’s important to recognize that although different stakeholders have different challenges around uncontrolled information growth and sprawl, the root cause of most information governance problems are the same. The good news is that an information governance strategy can serve as a rallying cry to help build consensus internally among the different stakeholders. That gets the organization as a whole moving in the right direction and helps open up budget so everyone can begin solving this root problem together.

**Kennedy:** The other big challenge is justifying the funding and being able to put the business case together. Quite often we hear that there is frustration when a policy or mandate comes out without funding attached to it. But we have worked with a lot of agencies, and there are a lot of saving opportunities under the information governance umbrella. Agencies that have been able to deploy some technology tend to be ahead of the game, because they can start to show results earlier in the process. Once you have a win under the belt it’s easier to go back to the organization and show the benefits in black and white – how much money was saved or how much risk was reduced. That can help you obtain
data management and have the confidence that they will work together as technologies and requirements change. Take eDiscovery as an example. There are lots of point solutions on the market to address specific parts of the eDiscovery process, but the market has matured to the point where there are also end-to-end products that are integrated and work together. We’re going to see the same thing happen in the security space and eventually in the data management space with recordkeeping. You’ll see these technologies start to converge and become more integrated. So make sure you are investing in technologies that are already integrated, or the companies you’re working with have solid roadmaps that are focused on integrating these different technologies. No organization has the time, resources, or money to manage a handful of different technology solutions and keep swapping out new point solutions for others.

Secondly, don’t lose sight of the fact that taking this modular approach to solving problems doesn’t mean you shouldn’t be considering a longer-term strategy for the organization. As an example, there are hundreds of different point solutions to address different specific data security, data management, and eDiscovery challenges, and the market is evolving at a rapid pace. That means it’s important to invest in technology solutions that are already integrated or have solid information governance integration roadmaps. Most organizations simply don’t have the time or money to continue to support multiple point solutions and can’t swap things out every year or two, so the long-term vision is very important.

Kennedy: Another factor that can make a big difference in the success of such an overarching initiative is properly training people within the organization on security, eDiscovery, and record-keeping procedures. You can have all of the technology and best intentions, but if people don’t understand what’s expected, you’ll only get so far.

Is there a time-critical element to developing a comprehensive information governance strategy?

Kennedy: Complying with federal mandates is a huge driver for getting things rolling, because there are a lot of milestone dates. Agencies that miss those dates will end up incurring financial penalties. Also, the sooner the information governance plan is operational, the sooner agencies can begin reducing risk and saving money.