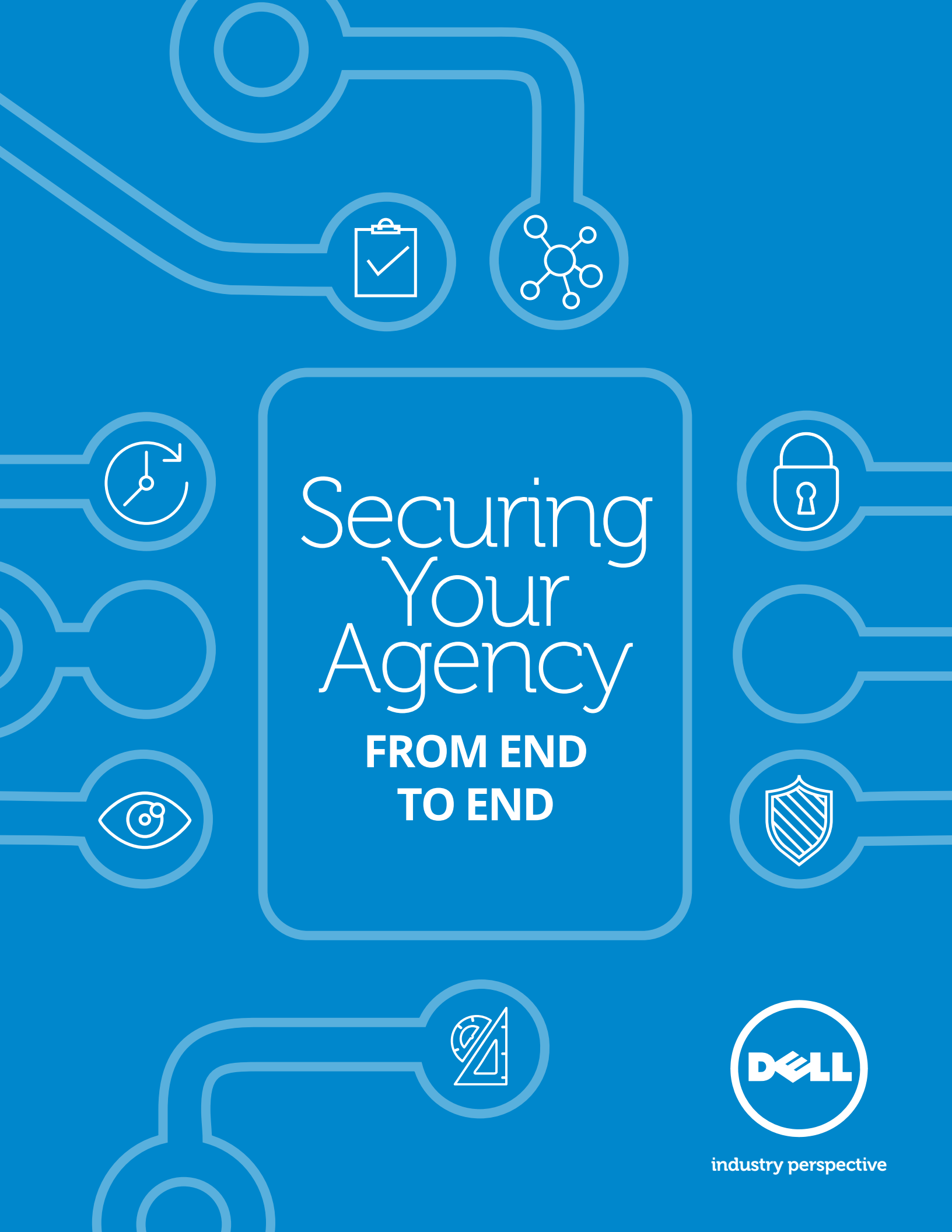

Securing Your Agency

FROM END TO END

industry perspective

A Tale of Cybersecurity in Government

Gone are the days when cybersecurity was just an information technology problem. In 2015 alone, eBay, LivingSocial, Adobe, Evernote, Home Depot and JPMorgan Chase joined the ever-growing list of companies facing major security breaches. And it's not just about compromised data: The breaches also amount to millions, if not billions, of dollars in lost revenue, poor customer satisfaction and embarrassing headlines. And if government officials were hoping to stay out of the fray, they were in for a rude awakening.

In April 2015, news broke that personally identifiable information on more than 21.5 million federal employees, contractors and applicants had been compromised because of a hack of the Office of Personnel Management. OPM estimated it will spend more than $133 million in the next three years to provide identity theft protection services to the victims.

And although the OPM breach marked the single greatest loss of information by a government agency, it was just the latest in a string of other government breaches. All of these attacks have brought security to the forefront of federal officials' attention. And while there is no quick fix, the need for an end-to-end solution is overwhelming, because as the breaches show, security is everyone's problem — not just IT's.

The good news for agencies is that there is help. From intrusion detection to application security to identity and access management, Dell is focused on implementing a holistic best-of-breed set of cybersecurity solutions. "Dell is a one-stop-shop for security solutions," said Paul Christman, Vice President of Federal Markets at Dell Software. Christman sat down with GovLoop for an in-depth interview to talk about Dell's holistic approach to cybersecurity.

In this report Christman will discuss:

1. **Dell's Future Ready Security approach.**
2. **The critical importance of identity and access management.**
3. **How to maintain endpoint security.**
4. **How to protect data effectively.**
5. **How to achieve effective perimeter security without sacrificing performance.**
6. **How to deal with agency-specific requirements.**
7. **Why metrics matter.**

A Dell tech security survey found that 84 percent of federal government agencies list information security as a top priority, compared with only 48 percent in the private sector. "Information security is nearly two times as important in the public sector right now as compared to the private sector. It's really important for agencies to take security seriously, and we want to enable that mission for them," Christman said.

In this report, we will tell you how federal agencies can and should prioritize their cybersecurity initiatives.

Future Ready Security

Transforming an agency's security posture is not an easy feat.

But Christman cautioned that in order to prevent future catastrophic breaches, a change is not just necessary, it's mandatory. "A passive defense is an old-school mentality that says, 'If I patch known vulnerabilities, if I update my virus signatures, or if I'm tracking malware, then my system is secure,'" he said. "That's wrong. The passive system is designed to address only the things that we already know about. It doesn't address things that we don't know about."

Enter Dell's Future Ready solution. Future Ready is not about certifications or checkboxes; it's about a risk-based, context-aware, flexible security solution. "It's what I call an active defense," explained Christman. "It's a much more proactive approach to understanding what's going on, rather than just responding to things that we've already seen before."

And with the emergence of cloud computing, mobility, big data and the Internet of Things in the government space, agencies need a solution that optimizes the differences between traditional and new applications. With Future Ready, agencies can proactively project everything from the device to the cloud with context-aware security services that predict, detect and stop cyberattacks.

"If you think about the concept of Einstein [a government intrusion-detection system] as a set of tools, it's really getting into that idea of examining users for anomalous behavior as opposed to looking for malware signatures," Christman said. "That's an example of where we're moving into this active defense."

Additionally, mandates are requiring agencies to reduce costs while still advancing government efficiencies. Securing a move to the cloud can do that. "The cost of 'do nothing' is higher than the cost of 'do something.' There are cost-effective ways to improve user awareness and security. For instance, simple annual training is a great first step," explained Christman. "You can do online, computer-based training that elevates awareness and reminds people you can do things that are cost effective to educate users."

Identity & Access Management

One of the biggest sticking points for cybersecurity professionals is figuring out who should have access to information — and when.

To make matters worse, bad actors are often the most successful when they gain access to a privileged user's username and password. Dell One Identity solutions for identity and access management (IAM) help agencies simplify and become agile while also addressing identity and access management challenges.

So how does it work? To better understand identity and access management, you first need to forget the idea that access is binary. Identity and access management really needs to have different access levels for people who have elevated privileges.

"We're doing a lot of work with a lot of different agencies across the entire federal government around very granular, very stringent forensic tracking of what happens with privileged accounts," Christman said. "We're getting to the point now where we can implement privileged accounts that have actually no username and no password. Privilege is granted ad hoc, as the access is needed. It's tracked, but there are no usernames and passwords exposed, so you don't have the exposure and the risk of reusing usernames and passwords or sharing usernames and passwords because we've reached the point where the password doesn't even exist."

Identity and access management marks an evolution for the most important credentials inside the network. With everyday users, Dell has created and integrated a two-factor authentication process, which would be a username and password plus a token, a Personal Identity Verification (PIV) card or Common Access Card (CAC) derived credentials. This way the access is granted based on the role and privilege level.

To keep costs down, Christman suggests that agencies create interoperable identity management system solutions. "The idea of having an identity that's tied to an application leads to enormous expense as well as poor security in the aggregate. One of the things we really recommend is Identity-as-a-Service. With Identity-as-a-Service, your identity is transferrable and applicable to grant appropriate access to multiple applications. Think about it as a service rather than something you have hard code it in every application. Identity-as-a-Service reduces your expense and improves your security profile."

Endpoint Security

Gone are the days when you saved all the important files on one hard drive on one computer in one data center.

Now, users want to access information from their smartphones, tablets and laptops. Work is literally mobile. This can create major challenges for cybersecurity professionals.

"I'm looking at my desk right now. I've got my laptop plugged into my docking station and I've got my smartphone and tablet next to it. The idea of a fixed workstation is so 1990," Christman said. "The good news is that Dell has a framework that explains how to manage an endpoint device, whether it's Android, iOS, a Windows phone or a tablet. It's all the same."

The techniques and protocols don't distinguish between a fixed desktop machine and a mobile smartphone running Android. Dell's latest next-generation firewall technology provides context-aware security across highly distributed networks.

Instead of thinking of securing data in one place, Dell's tools secure the device when it is requesting data, storing data and being granted access to data. "We have very robust tools to help do endpoint management rather than Windows device management," Christman said.

And government is taking notice. "I think the government's coming around to simple things like OS patch management — or acquiring, testing and installing patches. Agencies are coming around to the idea that they need to extend that same discipline and IT rigor to the endpoint devices, because the endpoint devices are what's being compromised."

Take a patch management upgrade, for example. Most often with patch management upgrades the challenge is testing for application compatibility. If users' applications don't run after they update their operating systems because somebody in IT didn't test application compatibility before authorizing and distributing the patch, that's a problem. "Those are the times when users get really cranky — when their machine reboots and then they can't get access to what they need to do their job. People think the IT guys disabled their mission work," Christman said. "With our tools, that doesn't happen. You don't get that disruption to your work."

Protecting Data

At its most basic level, cybersecurity boils down to protecting data.

Data is what powers the government and it needs to be protected both at rest and in transit. And even more importantly, data needs to be managed effectively in both places.

By incorporating data management policies at an early stage, agencies can focus their planning efforts on those services and assets that cloud delivery will most enhance or streamline.

But there is no one-size-fits-all data management strategy. "Data management is different for every single organization, but at Dell, we have created a framework — a way of defining what risk is to a particular organization, depending on what they're trying to protect and what they're trying to protect from," Christman said.

The Dell method of data protection flips the script on the traditional approach to securing information. "We are trying to encourage folks to look at security not just as a way of telling the user, 'No, you can't do this,' or 'You have to install that,' or 'You have to have another password.' The [telling people] no model doesn't work — the no model doesn't move the business forward," Christman said. "It may make you feel more secure, but eventually the no model stops working because users will find a way around the restrictions."

Dell noted in a white paper that the security posture must enable the business and must be something that consumers are actually going to use.

In addition to the framework, Dell trains its government partners to create what it calls the human firewall. "Users are one of the most important defenses we have. A human firewall is a community of users that understand their role in preserving the integrity, access and quality of data. They participate in the security process," Christman said.

At the end of the day, users have to buy into their part of the security execution. IT can do only so much — so that's where the human firewall and effective data management come into play. "You can only make a user so secure," Christman said. "What they really need to do is participate, willingly, actively, enthusiastically, and understand that cybersecurity is just part of the job."

Network Security

Currently, 25-35% of enterprise network traffic runs over SSL/TLS, and is increasing about 20% per year. According to Gartner, 50% of all inbound/outbound attacks will use SSL/TLS by 2017, up from 5% in 2013.

To protect against these threats, next-generation firewalls intercept the keys exchanged during the SSL process, using them to open and decrypt SSL traffic to look for threats. Network traffic is then inspected for questionable activity before being re-encrypted and sent to the recipient. This is a six step process, which according to NSS Labs, causes a performance loss as high as 81%.

To eliminate this performance hit and enable the traffic speeds demanded by federal agencies, Dell developed a massively scalable approach to network security which delivers strong performance and security at a low TCO.

"Firewalls by nature have historically been a choke point on the network", said Christman, "but Dell's Reassembly Free Deep Packet Inspection (RFDPI) and multi-core architecture, combined with Dell's Firewall Sandwich design, facilitates network speeds in excess of 100 Gbps." Christman also noted that Dell has equally effective firewall solutions for branch offices. A recent survey conducted by i360Gov.com revealed that nearly 90% of federal IT executives are concerned about data insecurity at remote or branch offices; 31% of survey respondents said their organization had experienced a remote office breach within the last 12 months.

The evolution of network security requirements, along with increasing traffic levels and the adoption of 40 Gbps and higher core networking technologies, have driven the industry to respond with ever larger, more complex, power-hungry and expensive solutions. Dell SonicWALL offers an alternative solution that addresses security, resiliency and performance requirements while reducing costs — a winning combination.

Agency-Specific Standards

There are more than 275 federal National Institute of Standards and Technology 800-53 security standards.

Add in federal mandates such as the Federal Information Security Act and the Defense Information Assurance Certification and Accreditation Process, and Federal Risk and Authorization Management Program (FedRAMP) compliance requirements such as Federal Information Processing Standard (FIPS) 140-2, and government workers can feel like they are swimming in security regulations. They're not wrong.

"Certifications are expensive, challenging and very valuable," Christman said. "So the burden on us as technology producers, manufacturers and publishers is to really make sure that we are addressing the most critical ones. Right now nobody satisfies all the requirements. We pick the most important ones."

For starters, Dell has decided to focus on three key requirements: FedRAMP for cloud, FIPS for encryption and Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) for interoperability and information assurance certification.

1. **FedRAMP Cloud:** The multitenant, secure FedRAMP cloud allows government users immediate access to FISMA Moderate resources to engage them to migrate secure workloads easily.
2. **Flexible Encryption:** Dell's flexible encryption supports the highest level of FIPS 140-2 protection commercially available for system disks.
3. **Interoperability and Information Assurance:** Dell SonicWALL SuperMassive 9000 series and Network Security Appliances have been UC APL certified for the device types of Data Firewall (DFW), Intrusion Protection Systems and Intrusion Detection Systems (IPS and IDS).

However, Christman cautioned against taking a solely compliance-based approach to security. Instead he recommends a holistic approach. "The idea that you are better off if you have more checkboxes is a false sense of security," he said. "The best thing that we can do is to understand what we're trying to protect and from whom and then invoke the right protocols. After the OPM breach, everybody was running around saying encryption would have solved the problem. Encryption wouldn't have solved the problem. It's such a kneejerk reaction to say encrypt everything and therefore you're more secure."

To facilitate agencies' security and compliance needs, Dell has launched a round-the-clock security operations center and network operations center to support IT staff and end users. "Security breaches don't just happen between 9 [a.m.] and 5 p.m.," Christman said.

Why Metrics Matter

One of the ways Dell is creating a robust cybersecurity culture is by looking at metrics.

"At Dell, we don't like to just show you how many breaches have been thwarted, we like to take things to the next level," Christman said. "And we have the metrics to back it up. We employ white hat hackers, whose job it is to try and break into your system."

The white hat hackers provide an assessment of how well agencies are protecting their data and how effective the data protocols are.

"You've got to measure it because you've got to show that you're actually doing this security thing for a reason," explained Christman. "And more importantly, if you set up a trap and you never catch anything, maybe the trap's not the in right place or maybe the trap's not looking for the right thing. Agencies need to make sure that they're actually achieving those objectives and in a very measurable way."

With Dell's robust tracking services, government officials can truly see how their cybersecurity initiatives are working.

"At Dell, we don't like to just show you how many breaches have been thwarted, we like to take things to the **next level**. And we have the metrics to back it up."

Paul Christman
Vice President of Federal Markets, Dell Software

The Security of the Future

Although there is no one cybersecurity silver bullet, there are ways to both anticipate and prevent attacks like the one launched on OPM's personnel records — as long as you have the right tools and processes.

"You have to arm your agency with the right mindset to both look back at historic trends and to the future to really create a holistic view of cybersecurity," Christman said.

Dell's security mission focuses on protecting, enabling and complying with government standards to create a true security solution. And if agencies use the information and technologies Dell provides, along with leveraging the essential guidance provided by the NIST Cybersecurity Framework, they could build not only a more secure future, but a safer one, too.

"We don't have to be behind the ball when it comes to cybersecurity," Christman said. "The government can be a leader, and with the right tools — like the ones we provide — your agency can be much more secure."

"We don't have to be behind the ball when it comes to cybersecurity. The government can be a leader, and with the right tools — like the ones we provide — **your agency can be much more secure**."

Paul Christman
Vice President of Federal Markets, Dell Software

About Dell

Dell empowers countries, communities, customers and people everywhere to use technology to realize their dreams. Customers trust us to deliver technology solutions that help them do and achieve more, whether they're at home, work, school, or anywhere in their world.

www.dell.com

About GovLoop

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 200,000 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 email us at: info@govloop.com

www.govloop.com

@GovLoop

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

Phone: (202) 407-7421 Fax: (202) 407-7501

www.govloop.com | @GovLoop