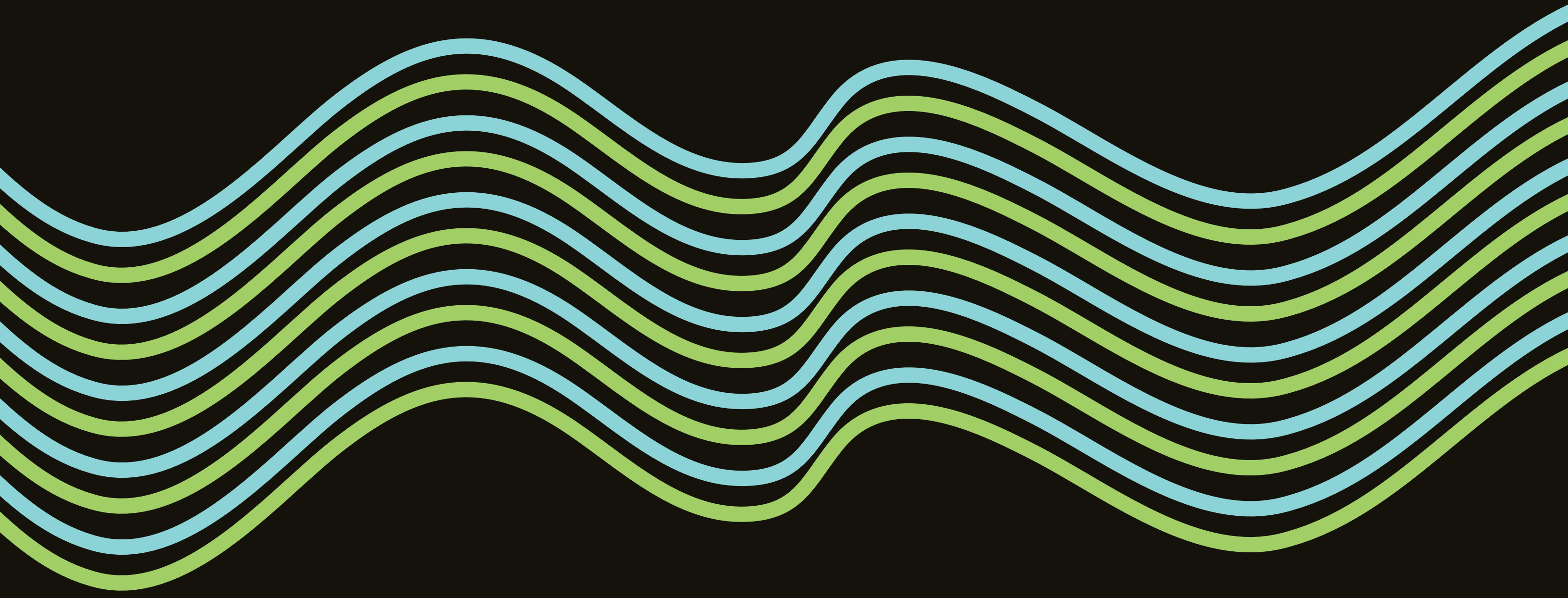

The Future of Government Cybersecurity

RESEARCH BRIEF

Executive Summary

During 2015, federal departments **collectively reported** 77,183 cybersecurity incidents, a 10 percent increase from 2014. Looking ahead, cyberrisks and attacks are rapidly increasing and evolving. In short, more clearly than ever, cybersecurity is everyone's priority.

Despite these increases, however, there does seem to be a silver lining: government is getting better and more capable at responding to cyberattacks. GovLoop partnered with Akamai, a leader in content delivery network services for advanced cybersecurity, to survey more than 350 federal employees and gauge the current state of cybersecurity in government as well as future trends.

For participants, the survey was intended to be a 2016 cyber year in review while gauging what's ahead for 2017. The survey addressed everything from agencies' top security priorities to agencies' top security concerns as well as primary approaches to mitigate threats. In order to gain a better understanding of the survey results and expertise from the private sector, GovLoop also interviewed Tom Ruff, Vice President of the Public Sector-Americas at Akamai.

The results showed that agencies are optimistic for the future and in their abilities to handle cyberthreats. Approximately 47 percent of those in agencies who suffered data breaches felt they were effectively able to respond (Figure 2).

While it's important to note that government is significantly improving in cybersecurity efforts, it's equally important to acknowledge persistent challenges. At least half of the surveyed respondents said cyberattacks, hacks and general security risks are increasing at their agency (Figure 3).

This research brief will outline the main findings from the survey results. Additionally, it discusses specific areas where government is making improvements in cybersecurity, areas that need improvement, strategies to address the challenges, and security best practices from the Department of Defense.

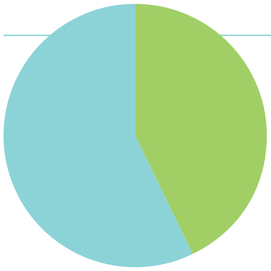

FIGURE 1

Did your agency suffer from a hack, data breach or cyberattack in the past year?

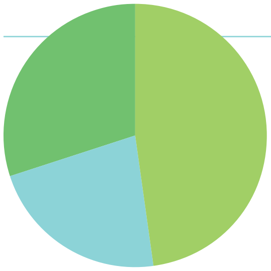

FIGURE 2

If yes, were you able to respond effectively?

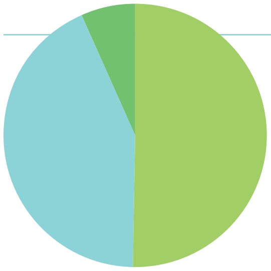

FIGURE 3

From 2015 to 2016, did cyberattacks, hacks, and general security risks increase or decrease at your agency?

Government's Improvements in Cybersecurity

There is a bright side to the rapidly increasing complexity and volume of cyberthreats: government is steadily getting better at handling them.

As part of the Obama administration's FY 2014–FY 2017 **Cybersecurity Cross Agency Priority (CAP) Goal Report**, agencies were measured on their improvements in Information Security Continuous Monitoring (ISCM); Identity, Credential and Access Management (ICAM/Strong Authentication); and Anti-Phishing and Malware Defense (APMD). At least 14 major civilian agencies improved in strong authentication. Agencies increased strong authentication use for privileged users from 33 percent to 75 percent.

Additionally, agencies made significant progress in the percentage of civilian users with Personal Identify Verification (PIV) cards (42 percent use to 81 percent) in 2015. The number of agencies that improved anti-phishing and malware defense went from 10 to 19 during the same year.

Federal government's progress in legislation and priorities is being reflected in agencies. Nearly 80 percent of survey participants felt their agencies were able to respond effectively or adequately to attacks they did suffer (Figure 2).

In addition to feeling better prepared, agency employees are also more aware about mobile security risks than ever before. Over 65 percent of respondents said they updated their security strategy to include mobile security protections (Figure 4).

Such improvements demonstrate that government is taking cyberthreats seriously. "Government has been doing a great job in making cybersecurity a priority," Ruff said. "Agencies are prepared as much as they can be, given the rapidly evolving landscape."

Agencies are taking more steps to move as quickly as possible to stay ahead of the growing threats.

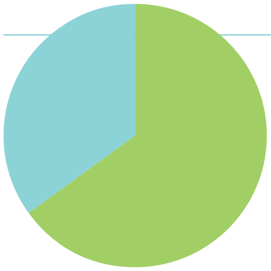

FIGURE 4

These days more agency employees are mobile than ever before. Has your agency updated their security strategy to include mobile security protections?

🟩 YES 65%　🟦 NO 35%

> "Government has been doing a great job in making cybersecurity a priority. Agencies are prepared as much as they can be, given the rapidly evolving landscape."

Tom Ruff, Vice President of the Public Sector Americas, Akamai

Persistent Challenges in Cybersecurity

There are many reasons for government to be optimistic for the future when it comes to cybersecurity. However, the survey results showed that many federal employees are only cautiously optimistic, with more than 47 percent of respondents admitting that they are worried about data breaches going into 2017 (See Figure 5).

Ruff affirmed that such concern is merited. "The number of the threats, the type of threats and the number of actors playing in this marketplace have only grown," he said. "And these threats have grown more serious in nature where you have nation states or organized crime perpetrators trying to profit from cyberattacks."

According to our survey findings, there are three major challenges for government in cybersecurity.

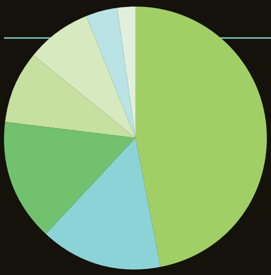

FIGURE 5

What is your number one cybersecurity concern going into 2017?

🟩 DATA BREACHES OF SENSITIVE INFORMATION 47%

🟦 PHISHING 15%

🟩 WEB APPLICATION ATTACKS 14%

🟩 RANSOMWARE 9%

🟩 OTHER 8%

🟦 DDOS ATTACKS 4%

⬜ SQL INJECTIONS 3%

Challenge 1: Sophistication of Threats

The most concerning challenge, according to survey results, is the increasing sophistication of cyberthreats. As Ruff said, the players and the sizes of attacks are getting bigger. There are new types of ransomware where hackers can hijack data and ask for payment with the threat of releasing sensitive information to the public. There are attacks that can shut down entire government infrastructures and attacks that can take days for agencies to detect.

All of these types of attacks can have a significant impact not just on government, but on the general public as well. **DHS noted** there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

Ruff emphasized that one particular threat that is becoming more important because of its sheer size and impact is Distributed Denial of Service (DDoS) attacks. Sixty percent of survey respondents affirmed that they were particularly concerned about DDoS (Figure 6).

DDoS attacks are malicious attempts to render a web site or web application unavailable to users by overwhelming the site with an enormous amount of traffic, causing the site to crash or operate very slowly. While DDoS attacks are one of the oldest types of threats against websites, they are constantly evolving, making it harder to defend against them. Today, attackers use large armies of automated "bots" – computers that have been infected with malware and can be remotely controlled by hackers – to create DDoS attacks on a very large scale.

Additionally, DDoS attacks are often used as decoys to divert the attention of IT teams away from other simultaneous attacks. Even the largest enterprises today find it nearly impossible to build out sufficient infrastructure to scale in response to a large DDoS attack.

"DDoS is becoming more important because the size of attacks that we're seeing could absolutely cripple any enterprise," Ruff said. "Two to three years ago, the average size of a DDoS attack was around 30 to 40 gigabytes. Now, they can exceed 120 gigs. There's no infrastructure that government could afford to put in place that could stop that size of attack, so it has a crippling effect."

DDoS is just one example of the evolving sophistication of cyberthreats. "The landscape is ever changing," Ruff said. "It's not a set [your solutions] and forget type of environment. Government has to keep innovating and being proactive. You're going to get an attack no matter where you are. What you have to realize is that you're not going to be able to protect everything. So do an assessment of what systems and apps would have the biggest implications and protect those first."

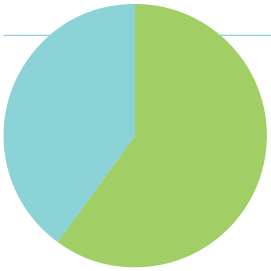

FIGURE 6

Are you concerned about DDoS (Denial-of-service) attacks?

🟩 YES 60% 🟦 NO 40%

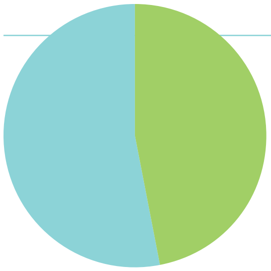

FIGURE 7

Is more budget being dedicated to cybersecurity at your agency in the next year?

🟩 YES 47% 🟦 NO 53%

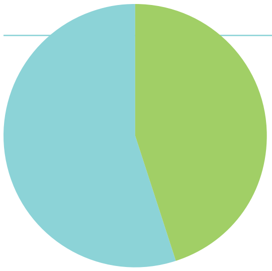

FIGURE 8

Are the risks of cyberattacks widely understood at all levels of your agency, even beyond IT and security?

🟩 YES 44% 🟦 NO 56%

Challenge 2: Resource Constraints

In addition to tackling the increasingly sophisticated level and volume of cyberattacks, government struggles with shrinking budgets and an inability to draw advanced IT professionals into the workforce. Moreover, government does not necessarily have the freedom to direct IT funds where they're really needed.

Approximately **three-quarters of all government IT spending** is going to support legacy systems (computer systems or technologies that are often out of date or need replacement). When GovLoop's survey respondents were asked if more agency budget was being dedicated to cybersecurity in the next year, more than half said "no" (Figure 7).

That's not surprising. "Agencies need to do more with less," Ruff said. "Government is using contractors to supplement the current IT population, but hiring security expertise becomes very difficult for government in light of competitiveness with the commercial world."

This is why it has been said that the fiscal 2017 budget is at a **"make or break"** point for cybersecurity and the federal government. The 2017 president's budget request asks Congress for $19 billion to support a broad-based cybersecurity strategy for enhancing critical infrastructure. This is a 35 percent increase in the 2016 budget.

This money will largely be used to support the **Cybersecurity National Action Plan** and its associated directives. CNAP takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections. Other appropriations within the proposal, however, indicate additional cybersecurity priorities at the federal level. Recognizing a need to further explore innovative technological solutions to cyber challenges, $318 million will be allocated to research and development investments at federal civilian agencies.

Additionally, the proposed $3.1 billion **Information Technology Modernization Fund** would help agencies retire legacy technologies and replace them with newer, more secure IT systems. The revolving fund will also be used to ensure agencies maintain critical systems not yet at the end of their lifecycle with appropriate security measures.

But the budget challenge remains imminent as the funding under the above-mentioned initiatives is anything but guaranteed. Despite hope for future cybersecurity and IT investments, government will have to be prepared to attempt massive IT modernization efforts within the next year without further funding.

Challenges 3: Lack of Education in the Cyber Workforce

One huge hurdle in cybersecurity for government is over dependence on IT teams to take care of the problem. Agency-wide staff are often unaware of what to do during cyberattacks. They are also increasingly vulnerable to becoming insider threats at their own agencies by being uneducated about safe cyber practices. Over 56% of survey respondents said cyberattacks were not widely understood at all levels of the agency, even beyond IT (Figure 8).

Beyond technical skills, simple management and daily use of IT systems is ripe for misuse. As tools diversify, employees often seek ways to streamline and integrate these technologies with their workflow. That can result in workarounds – things like writing down passwords, sharing accounts or even adding new, unsecure technologies that increase productivity at the cost of security.

"The number one threat for cyber happens to be our employees," Ruff said. "So it really centers around cybersecurity hygiene."

Additionally, due to evolving and increasing cyberthreats, traditional IT or general service skills are no longer enough to keep government secure. **Fewer than 25 percent** of cybersecurity applicants are qualified to perform the skills needed for the job.

What's more, government is having trouble accruing the talent it needs. This is especially true as it competes with the private sector to fill critical cybersecurity positions, due to lower pay and longer time-to-hire in government. The rate of growth for jobs in information security is projected at **37 percent** from 2012 to 2022. The workforce is expected to grow at a compound annual growth rate of **11.3 percent globally** between now and 2017.

While the technical, resource, and workforce challenges in government cybersecurity are significant, there are many ways government can overcome these obstacles.

"At the end of the day, the challenges are only part of the story," Ruff said. "What organizations need to do is have more in-depth approaches like advanced authentication, endpoint security, and real-time cloud solutions that can take on the threats. Government also needs to make sure employees know cybersecurity and the impact of security programs."

Strategies and Tools to Help

Government can use three primary strategies to address the challenges to cybersecurity: continuous monitoring and advanced authentication; cloud-based platforms; and improved employee education and hiring tactics.

Solution 1: Continuous Monitoring and Advanced Authentication

Going forward, government needs to look at ways to improve how users are managed while monitoring and maintaining security systems to prevent future cyberattacks. Advanced authentication and continuous monitoring paired together can help government better manage who's accessing what important information within agencies while making sure that cyberthreats can be detected ahead of time.

With two-factor authentication, agencies can better mitigate external and insider threats by making it more difficult to steal identities or access important information. An advanced authentication solution can allow you to set different use policies and controls for different users. For example, agencies could set up a policy that requires one specific team to complete two-factor authentication only once every 30 days, as long as they log in using a trusted device or network. This is more convenient for users who don't have privileged access to sensitive information; ensuring quick, easy and secure access.

In addition to advanced authentication, agencies also need to take advantage of DHS's **Continuous Diagnostic & Mitigation (CDM) program**. The CDM program provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts and enable cybersecurity personnel to mitigate the most significant problems first.

Tools to help enhance the impacts of continuous monitoring and advanced authentication include site defenders. They can help by offering built-in scalability and global reach to help enterprises fend off large attacks, like DDoS, while protecting web applications from direct-to-origin attacks.

Site defenders can help maintain website performance and availability even when confronted with fast-changing threats, by providing:

- Adaptive rate controls that allow you to monitor and control the rate of requests against applications
- Network-layer controls for defining and enforcing IP whitelists and blacklists that allow or restrict requests from certain IP addresses or geographical regions
- Security monitor for real-time visibility into security events
- Logging tools to increase threat posture awareness

> What an agency needs are comprehensive security policy and the ability to monitor a robust and evolving security program. Cloud approaches give government enterprises a way to adapt and adjust."
>
> Tom Ruff, Vice President of the Public Sector Americas, Akamai

Solution 2: Cloud-based Platforms

Whether internal or external, users expect online experiences to always be available and secure and for their personal information to be safe. Cloud-based platforms can help protect government data without sacrificing performance for security.

Cloud monitoring platforms offer the ability to easily integrate transaction and security event data from multiple, disparate systems into a centralized reporting environment. Additionally, such platforms allow leaders to gain instant visibility to application usage across application portfolios, regardless of where the applications are hosted.

Agencies can enhance security with easier monitoring of detailed application performance, usage, and end-user experience for all applications in the cloud. Cloud monitoring tools and platforms can also help monitor web security events and incidents across your environment while gaining deep insights into application transactions.

As outlined in the President's 2011 **Cloud First Policy**, cloud computing has the potential to play a major role in addressing the inefficiencies in government's IT environment while improving government service delivery. Cloud computing platforms can help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints.

"What an agency needs are comprehensive security policy and the ability to monitor a robust and evolving security program," Ruff said. "Cloud approaches give government enterprises a way to adapt and adjust."

Solution 3: Improve Employee Education and Hiring

To address the cyber skills gap, agencies need to accelerate learning and skills development; diversify the cybersecurity community; and provide career development opportunities within the cybersecurity field.

The Department of Homeland Security (DHS) provides a **Cybersecurity Workforce Development Toolkit** to help better prepare them in recruiting and training their cyber workforce.

The toolkit is divided into four sections to help organizations understand where to start in assembling their cybersecurity teams:

1. **Assess Your Organization's Cybersecurity Workforce Planning Readiness.** Self-evaluation can help determine the readiness of your organization to conduct cybersecurity workforce planning.
2. **Plan for Your Cybersecurity Team.** Use tools to evaluate your agency's current and future cybersecurity workforce needs; explore your cybersecurity risks and find suggestions to close workforce gaps.
3. **Build Your Cybersecurity Team**. Identify roles that make up a great cybersecurity team; view cybersecurity talent profiles to help make informed hiring decisions and see tips for recruiting cybersecurity staff.
4. **Develop Your People.** Find templates to create custom cybersecurity career paths; links to training, certifications and professional events and ideas for retaining staff at every level.

But it's important to note that building an adequate cyber workforce in government will take serious time, energy and resources. To address immediate cybersecurity priorities, a combination of cutting-edge attack detection and mitigation technology enhanced by managed web security services can help make the job easier for IT teams and agency-wide staff.

Managed web security consists of outsourced services specifically designed to give agencies a proactive defense against data breaches, DDoS attacks, and the complete evolving landscape of emerging cyber threats.

Seasoned web security experts on a provider's security team can help detect and mitigate attacks. They can also act as web security consultants who ensure that web applications and network systems are always up-to-date and protected against emerging threats.

As government steadily recruits, builds and educate its cyber workforce, managed web services can supplement immediate cybersecurity needs for the time being. At the same time, government should not stop developing tactics to recruit and train more cyber professionals for the long-term.

Case Study: Department of Defense Launches Bug Bounty

When you are the federal government's largest agency, how do you uncover security weaknesses and vulnerabilities without jeopardizing the country's most critical systems and data? This was the idea behind the Defense Digital Service (DDS), an agency team of the U.S. Digital Service that strives to innovate the way DoD builds and deploys technology and digital services. DDS was charged with leveraging private sector talent and best practices to improve DoD's most critical services.

In early 2016, DDS convinced DoD to launch its first ever bug-bounty called "Hack the Pentagon." This was a cost-effective way for DoD to support its internal cybersecurity experts and better protect its systems and networks.

The Challenge

While bug bounties are common in the private sector, the federal government had never before implemented this approach. That said, the concept is relatively simple: an organization incents outside researchers – called white-hat hackers – to test the security of its networks and applications. Rather than exploiting those flaws, the hackers report what they find to the hiring organization so it can proactively address the vulnerabilities.

The U.S. Federal Government hired a third party, HackerOne, to organize and manage the hackers who would try to identify vulnerabilities. To ensure the success of this program, DDS worked closely with Defense Media Activity (DMA), which provides DoD enterprise-wide cloud services consisting of a web-based content management system for over 700 public-facing military and DoD websites.

Both DDS and DMA understood that inviting people to hack a federal agency was a little risky. But they also realized that the more hackers invited to participate, the more bugs the DoD would find. They also knew that to provide both experienced researchers and novice hackers with a meaningful challenge, the program needed to include sites that were significant targets along with some outside of the DoD perimeter.

The Goals

***DDS needed to meet two key goals to support its objectives*:**

1 **Thwart Internet-based attacks.**
DoD-related sites are high-visibility targets and the program would shine even more media attention on them, increasing the likelihood of attacks.

2 **Ensure availability.**
To get the most value possible from the hackathon, DoD needed to ensure the sites it offered up for vulnerability testing stayed online for hackers.

Outcomes

To meet these objectives, DoD engaged Akamai's services since defense.gov was already protected by Akamai. Since Akamai already has a bug bounty program in place for private companies to test their own systems, Akamai's experts could provide needed insights and suggestions for consideration throughout the program.

The Hack the Pentagon program ran from April 18 – May 12, 2016, during which time 252 vetted hackers submitted at least one vulnerability report, for a total of 1,189 reports. As the hacker reports were submitted, DDS worked to remediate them in real time with support from HackerOne. A little more than a month after the pilot finished, DDS had remediated each reported vulnerability.

One-hundred thirty-eight reports qualified for the bounty, and 58 of the 1,410 registered hackers received payouts ranging from $100 to $15,000. The total contract value, including the paid out bounties, was approximately $150,000. In the Secretary of Defense's estimation, DoD would have spent more than $1 million uncovering the same vulnerabilities if it had undergone its typical process of hiring an outside firm to conduct a security audit and vulnerability assessment.

In order to uncover the most vulnerabilities, it was critical that DoD maintained access to systems and online services during the hackathon. Akamai delivered and protected three of the five participating sites without interruption throughout the program while serving 213 million hits and 10 Terabytes of data, and absorbing traffic spikes of approximately 2,000 hits per second. Not surprisingly, the Bug Bounty program attracted attention from nefarious actors. For example, Akamai protected defense.gov against 55 sophisticated attacks with over 19.2 million malicious requests denied, including two notable DNS domain flood attacks, and a DDoS attack originating from 250 IP addresses in 83 countries.

What DoD's bug bounty demonstrates is that innovation is critical for government to take advantage of solutions like cloud, continuous monitoring and advanced authentication. Additionally, hackathons can help attract and identify more needed talent to the workforce, all while spending less and using resources more efficiently.

Conclusion

Government has many reasons to be worried about the future, but just as many reasons to be optimistic. While the sophistication of threats, constrained resources, and lack of education in the cyber workforce remain persistent challenges, there are many innovative solutions that government can use to overcome. Looking forward to 2017, government can look to continuous monitoring and advanced authentication, cloud-based platforms, and improved employee education and hiring tactics to tackle evolving cyberthreats.

"No government entity or enterprise can move as fast as adversaries are moving," Ruff concluded. "But government is moving in the right direction. A defensive strategy is continuing to educate, enforce policy, and make sure you have the budget."

About Akamai

Akamai is the global leader in Content Delivery Network (CDN) services, making the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere.

To learn more, visit: **https://www.akamai.com/us/en/solutions/industries/public-sector-cdn-services.jsp**

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 250,000 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**.

govloop

1152 15th Street NW, Suite 800 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop