

# **All Systems Back Online:**

**Maximizing Uptime, Performance, and Availability of  
U.S. Government Networks**

Sponsored by:



## THE BIG ISSUE

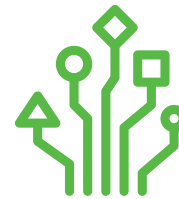
**Complex systems of networks and servers now power many of government's core services to the public and in our nation's defense. When these systems fail, they disrupt critical services and can sometimes even put human lives at risk.**

## THE STATUS QUO IS OBSOLETE



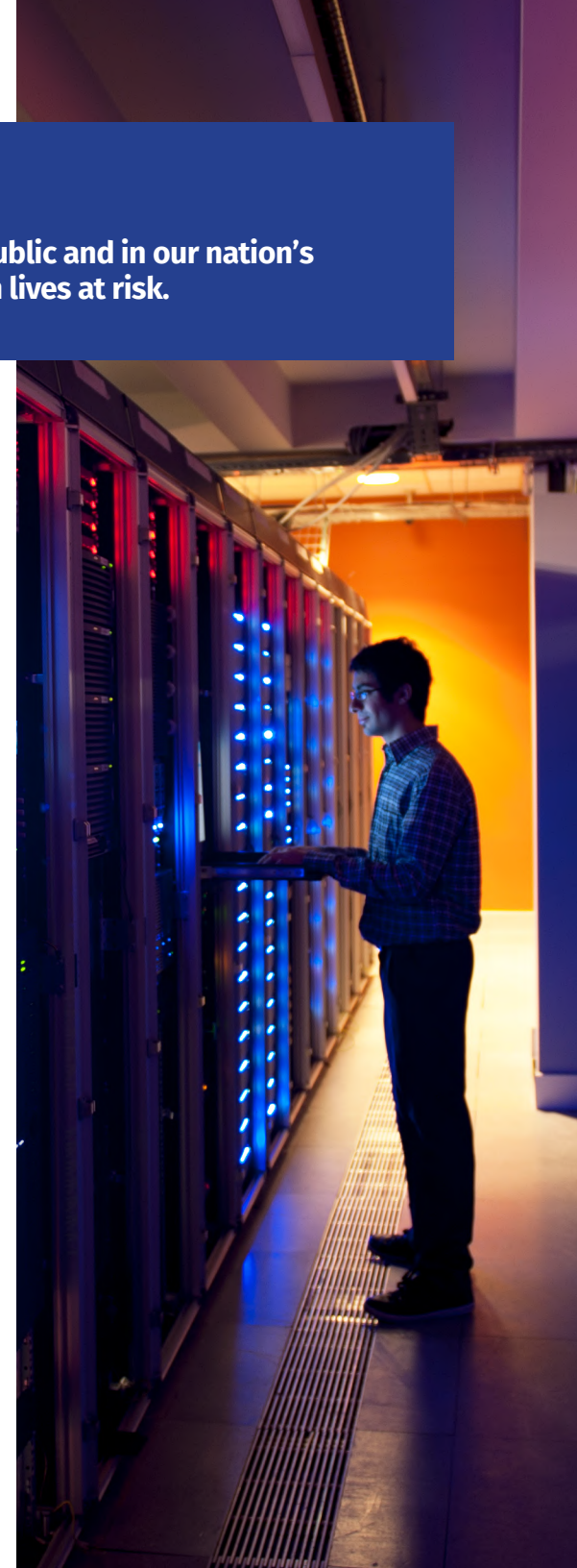
The public service mission means that when the systems powering critical services go offline, it can jeopardize timely service delivery and citizen experience and undermine public confidence in government-run entities.

To ensure mission success, government agencies must be vigilant about the reliability, availability, and performance of their underlying digital infrastructure.



Lack of end-to-end visibility across heterogeneous systems is a top concern among agencies who want real-time situational awareness and the agility to avert system outages before they take place.

Moreover, data complexity presents problems that current siloed IT systems are unable to address. When outages do occur, blame is distributed across multiple parties and root cause analysis takes too long.



## LACK OF SITUATIONAL AWARENESS PERSISTS ACROSS GOVERNMENT

### FEDERAL:

Due to an “internal systems failure,” the primary database hosting a majority of US Patent and Trademark Office (US PTO) systems went down for eight days in 2018, crippling electronic filing, patent application retrieval, and electronic patent assignment functions. While customers could submit paper filings, each submission cost users \$400 -- prompting many to turn to Twitter to express their disappointment.<sup>1</sup>



---

On the last day of the 2018 Filing Season (April 17, 2018), the Internal Revenue Service (IRS) experienced outages resulting from a firmware bug that caused a storage array to fail. As a result, 59 tax systems, including the Modernized e-File system, were unavailable for about 11 hours.<sup>2</sup>

### STATE AND LOCAL:

Vermont state government websites went down for six hours in August 2018, halting operations across multiple departments. Websites for the Secretary of State, Governor’s Office, Legislature, Attorney General’s Office, and the Department of Motor Vehicles were unavailable, disrupting email access and DMV license issuing.<sup>3</sup>



Just two weeks later, Iowa state government agencies also saw network outages take out websites used by Iowa State Patrol, Department of Transportation, Department of Natural Resources, and the Sex Offender Registry. Government users of the network include Iowa public schools, universities, hospitals, and medical clinics, all of which would have been affected by the outage.<sup>4</sup>

“Despite the impact of NIDEs [network/internet disruptive events], there is a lack of any rigorous understanding of internet outages or sufficient tools for their systemic and timely identification.”

- News Release, Department of Homeland Security (2018)





## THE BOTTOM LINE:

Agencies require real-time situational awareness through end-to-end visibility into the underlying infrastructure to ensure uptime, performance, and availability of critical services.

## PUTTING EYES ON THE NETWORK:

Fortunately, some organizations recognize the mission-critical urgency of the situation and are taking steps to bolster protection against IT-related disruptions.

- **Root cause research:** DHS recently awarded \$11.6 million in grants to organizations focused on protecting against massive disruptions to critical infrastructure. Programs include innovative approaches to real-time network monitoring, identifying taxonomies common to large-scale outages in public emergencies, root-cause attribution of NIDES, development of open-source tools, and evaluation of Application Programming Interfaces (APIs) that facilitate multiple system integration.<sup>5</sup>
- **Removing silos:** The Data Cabinet has released its Federal Government Data Maturity Model emphasizing the need for 'cross-functional prescriptive analytics'. The architecture calls for removal of data silos so that data can be managed according to agency-wide needs in a way that meets uniform standards of documentation.<sup>6</sup>
- **Connecting systems under one roof:** Advancements in monitoring and IT troubleshooting technologies now provide agencies with steps to bring previously disparate IT functionality all under one roof, without physically integrating them. By adding visibility and analytics, CIOs, CISOs, and teams spanning network, server, and cloud platforms have access to the same diagnostics tools, thus making root cause analyses and proactive mitigation of outages more achievable.
- **Hybrid environment:** As agencies increasingly embrace hybrid (on-premises and cloud) environments to deliver cost-effective yet secure services, cohesive monitoring across infrastructure and systems is critical.

## RISK OF INACTION:

Whether the mission is customer service or keeping the country safe, government agencies rely on a complex network of heterogeneous devices, systems, and applications. Currently, however, agencies lack the visibility to detect blind spots and troubleshoot (or even predict) potential issues, keeping them from delivering on their objectives. A recent study found that network downtime cost organizations on average \$5,600 per minute, or \$300,000 per hour, and significantly impeded employees' ability to refocus on their work following an interruption.<sup>7</sup>

As agencies look to consolidate IT and modernize systems, these challenges only exacerbate the problem. System downtime contributes to not only poor citizen experience but also lost productivity, tying up scarce resources in fire drills and overrunning agency budgets. In many cases, agency reputation suffers and can bring additional congressional oversight. With real-time visibility and analytics-driven insights, agencies can significantly improve their troubleshooting capabilities and ensure mission success.



## WORKING WITH SPLUNK

An agency's ability to measure, monitor, and optimize the infrastructure that supports its mission critical services has a direct impact on service delivery and citizen satisfaction. To ensure success of their missions, Splunk delivers real-time monitoring and predictive troubleshooting capabilities to maximize availability and performance of mission-critical systems and applications that support their initiatives.

With Splunk, you can:

- ➔ Increase probability of mission success by predicting failures and with fewer system outages
- ➔ Automate repetitive NOC procedures so scarce resources can focus on higher priority initiatives
- ➔ Accelerate investigation of system incidents by accurately pinpointing root cause and source of problems faster
- ➔ Improve efficiencies and reduce complexities by consolidating operational tools and/or external service

Splunk's solution is massively scalable, available, and easy to deploy on-premises or in the cloud because it enables fast and seamless ingestion and correlation of data regardless of source, type or format. It is easy to incorporate Splunk into an agency's dynamic environment and monitor key metrics and performance indicators providing IT staff the real-time situational awareness they need — no major implementation or resource burdens required.

## ENDNOTES

1. *The Register*: “Face-PALM: US Patent and Trademark Office database down for 5 days and counting.” August 20, 2018. [https://www.theregister.co.uk/2018/08/20/uspto\\_database\\_issue/](https://www.theregister.co.uk/2018/08/20/uspto_database_issue/)
2. Treasury Inspector General for Tax Administration: “Review of the System Failure That Led to the Tax Day Outage.” September 19, 2018. <https://www.treasury.gov/tigta/auditreports/2018reports/201820065fr.pdf>
3. *Burlington Free Press*: “VT government Internet outage: Service restored.” August 8, 2018. <https://www.burlingtonfreepress.com/story/news/politics/government/2018/08/08/vermont-government-loses-internet-access/934142002/>
4. *Des Moines Register*: “State government, agency websites go down Wednesday morning.” August 22, 2018. <https://www.desmoinesregister.com/story/news/local/2018/08/22/iowa-communications-network-icn-state-government-website-internet-outage-agency-department-dot-dnr/1063488002/>
5. DHS: “News Release: S&T Awards \$11.6M to Defend Against Network/Internet Disruptions.” September 14, 2018. <https://www.dhs.gov/science-and-technology/news/2018/09/14/news-release-st-awards-116m-defend-against-networkinternet>
6. Data Cabinet: “The Federal Government Data Maturity Model.” <https://www.ntis.gov/TheDataCabinet/assets/FDMM.pdf>
7. Gartner: “Blog: The Cost of Downtime.” July 16, 2014. <https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>

### Government Business Council

#### ABOUT GOVERNMENT BUSINESS COUNCIL

As Government Executive Media Group’s research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive’s 40 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at [www.govexec.com/insights](http://www.govexec.com/insights)

**Report Author:** Daniel Thomas



#### ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. More than 13,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises.

Learn more at [https://www.splunk.com/en\\_us/solutions/industries/public-sector.html](https://www.splunk.com/en_us/solutions/industries/public-sector.html)





Government  
Business  
Council

Sponsored by:

**splunk**<sup>®</sup>>