



The Open-and-Shut Case for a Cybersecurity Upgrade

In the past few years, government leaders have become more aware of the cybersecurity risks facing agency data, and have taken clear action to address the problem via mandates like the [National Cybersecurity Strategy](#), [secure supply chains](#) and [zero trust](#).

Following these mandates can go a long way toward enabling agencies to protect sensitive data and system access. Yet many agencies are bogged down in budget battles and lengthy procurement cycles, and saddled with legacy systems.

In this report, we will discuss:

- Effective ways to secure the environment and meet mandate requirements
- Why agencies should rely on modern, proactive cybersecurity technologies
- The importance of effective automation and monitoring



Challenge: A Growing To-Do List

Protecting data against cybercriminals has unique challenges in government:

- **A changing threat environment:** If your cybersecurity strategy can't adapt, your agency will fall behind and become an easy target for cyberattacks. What's more, hackers often assume that governments have inherently weak cybersecurity technology and strategies, making them easy marks.
- **Highly valuable data:** Social Security numbers, birth dates and drivers' license numbers, employee payroll information, banking and credit card information, court records, government research and state secrets—all of this information is highly coveted by hackers, who can sell it on the dark web.
- **Multiplying mandates:** Complying with multiple cybersecurity mandates is important, but it takes time, knowledge and money. Across the board, security leaders say keeping pace with security requirements has gotten harder over time.
- **A preponderance of legacy tech:** Older systems often remain operational because they are essential to government business. At the same time, these systems can be incompatible with modern security measures like multi-factor authentication, role-based access or some types of encryption.

"As agencies adopt more hybrid cloud infrastructures and take advantage of edge computing, the way data must be protected has changed."

Sam Deckel, Strategic Communications

Solution: A Prioritized Cybersecurity Upgrade Plan

Every agency has a cybersecurity plan, but it can easily become outdated. When it's time to update a plan, where do you begin?

A prioritized cybersecurity upgrade plan identifies the most important issues by weighing the impact of a security breach against the complexity of remediation. Critical steps of this process include:

- **Collect and aggregate information.** Gather and consolidate all relevant data and information pertaining to the security assessment: network logs, system configurations, vulnerability scan results, incident reports, etc.
- **Analyze, display and evaluate.** Map security and compliance standards to the environment and display them in an easy-to-understand way to enable effective evaluation. This step often includes data mining, statistical analysis and risk assessment methodologies. Evaluation involves assessing the severity and potential impact of the identified risks and prioritizing them based on likelihood and potential consequences.
- **Act.** Take actions based on evaluation results. This includes:
 - » End-to-end encryption, including at the edge, so when data is transferred to a data center or cloud, it's already protected
 - » Immutable (unchangeable) backups to protect data and enable agencies to recover quickly
 - » A full complement of security, identity and compliance, and advanced threat protection

Best Practices in Cyber Upgrades



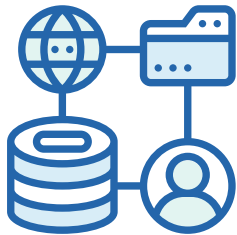
Implement Automated Audits

IT security audit tools can drastically cut down the time it takes to ensure compliance. For example, a 500-device audit performed manually takes 19,500 hours, versus 154 hours in an automated fashion. Make sure the audit tool you choose supports the compliance frameworks your agency depends on. Extra points if it provides monitoring and built-in remediation if an attack occurs.



Enforce Continuous Monitoring

Security threats change, and the only way to keep up with those changes is through continuous monitoring. While it's possible to do this internally, many agencies consider this work perfect for outsourcing. A good continuous monitoring team will use up-to-date network monitoring tools and provide accurate reporting and analytics, along with a plan to optimize network security.



Know Where Your Resources Are

Observability and visibility aren't set-it-and-forget-it. Agencies must always know where resources are, where they are being used and who has access to them. That means having a well-documented and up-to-date framework for the entire infrastructure, whether on premises or in the cloud, Deckel said. Keeping this information current is also the best way to ensure your devices aren't being accessed by unauthorized users and that specific users don't have too many permissions they don't need.



Speed Up the Procurement Process

Procurements often take longer than they should, and that's important when it comes to cybersecurity, where timing is everything. For much of government, the quickest path to procurement is working with a small, minority-owned or otherwise disadvantaged business, especially one with contract access and strong partner relationships. That's because government has specific goals about how many contracting dollars go to small, disadvantaged businesses, and that amount is set to increase with the Biden administration's commitment to grow that number by 50% by 2025.



Cyber Upgrades in Action

Here are three examples of agencies undertaking cybersecurity upgrades:

- A state agency responsible for all data center operations needed to replace its on-premises backup system to a cloud-based equivalent so it could employ immutable storage, which it considered necessary to improve cybersecurity. The idea was that it would work just as before, with other agencies in the state renting backup space, but the backups would now reside on Amazon Simple Storage Service Glacier (Amazon S3 Glacier), a secure service for **low-cost data archiving and long-term backup**. As a result, all agencies within the state can store backups for less than one cent per gigabyte per month and then backup and restore from immutable copies.
- With security being top-of-mind, a branch of the Defense Department (DoD) set out to find a better cloud management platform to meet its needs. The solution was an **image-based self-hosted platform** deployed via AWS Marketplace that ran directly and securely inside of the branch's existing Amazon Web Services (AWS) environment. This method gave DoD the data security and sovereignty it required, because no vendor ever touches or sees any DoD data. The platform also provided continuous compliance and cybersecurity monitoring, enabling the DoD to uncover risks and vulnerabilities like misconfigurations and policy breaches in seconds.
- Another branch of the DoD, looking to mitigate the risks of open-source libraries, Infrastructure as Code and other modern development tools, wanted more effective application testing. The solution was a **cloud-based application security testing platform** designed specifically for public sector regulatory compliance. The solution scans applications pre-launch for exposure to any of the latest cyber vulnerabilities, as well as regulatory compliance standards.

"Government is often seen as a softer target, but improving cybersecurity protection can help reduce that misconception."

Sam Deckel, Strategic Communications

How Strategic Communications and AWS Help

Strategic Communications is a one-stop shop for government cloud procurement. The team can provide public and private cloud resources, security applications, software and training all in one place. AWS provides economies of scale to drastically lower infrastructure costs. By deploying security solutions to the AWS Cloud, agencies get a scalable infrastructure that can match ever-changing IT landscapes. The collaboration also means that agencies get custom-designed solutions faster without sacrificing quality or expertise.

Learn more at <https://www.yourstrategic.com/aws>.

