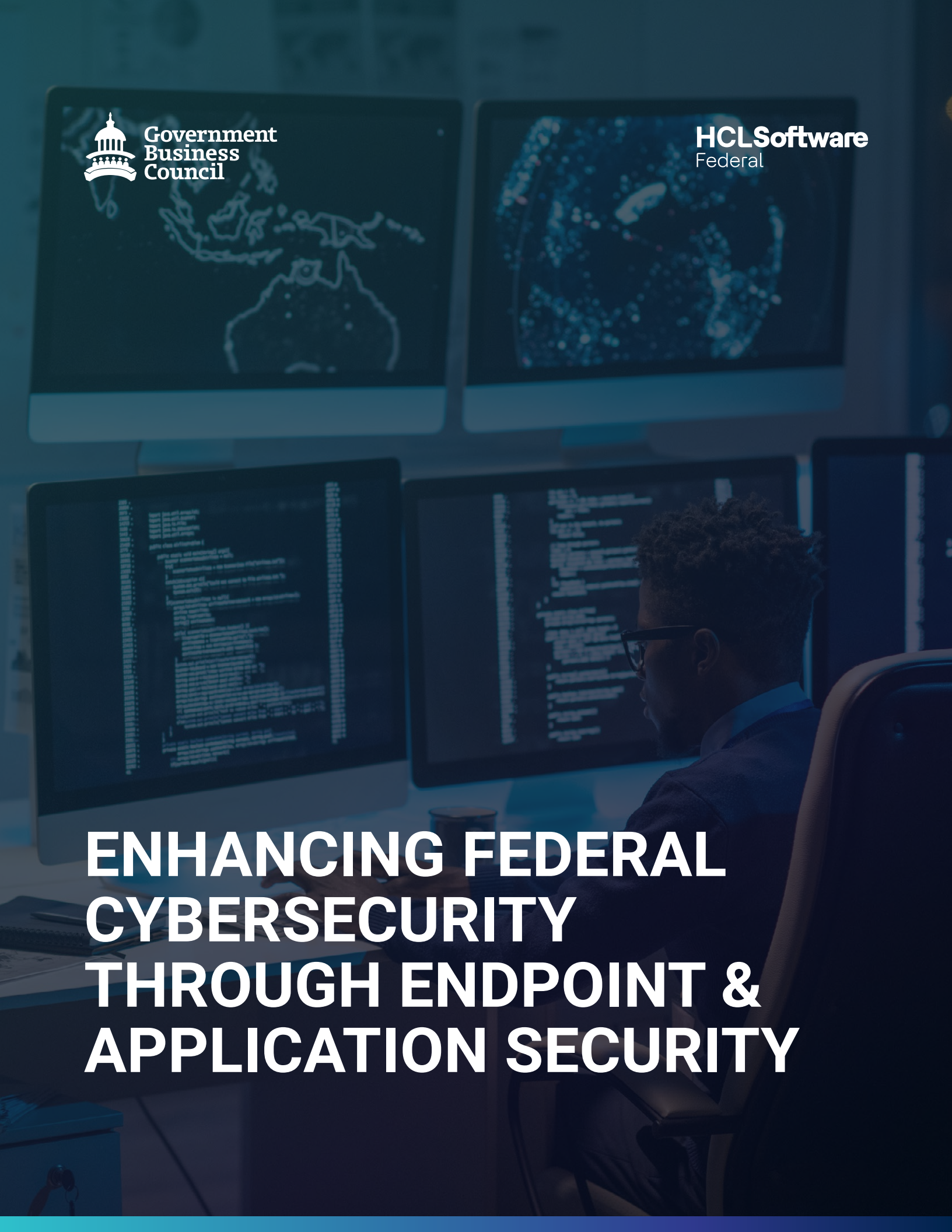


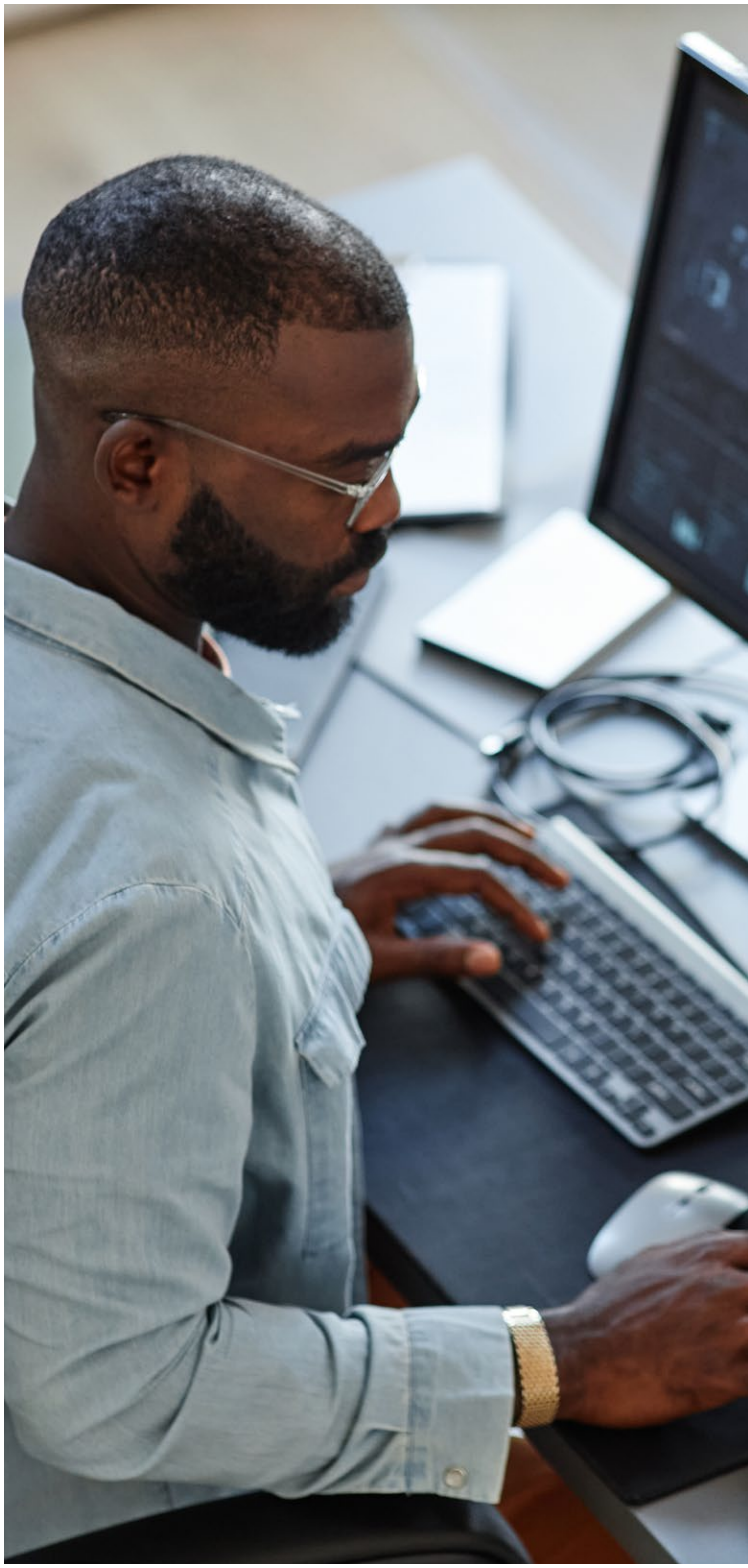
Government Business Council

HCLSoftware Federal

ENHANCING FEDERAL CYBERSECURITY THROUGH ENDPOINT & APPLICATION SECURITY

INTRODUCTION

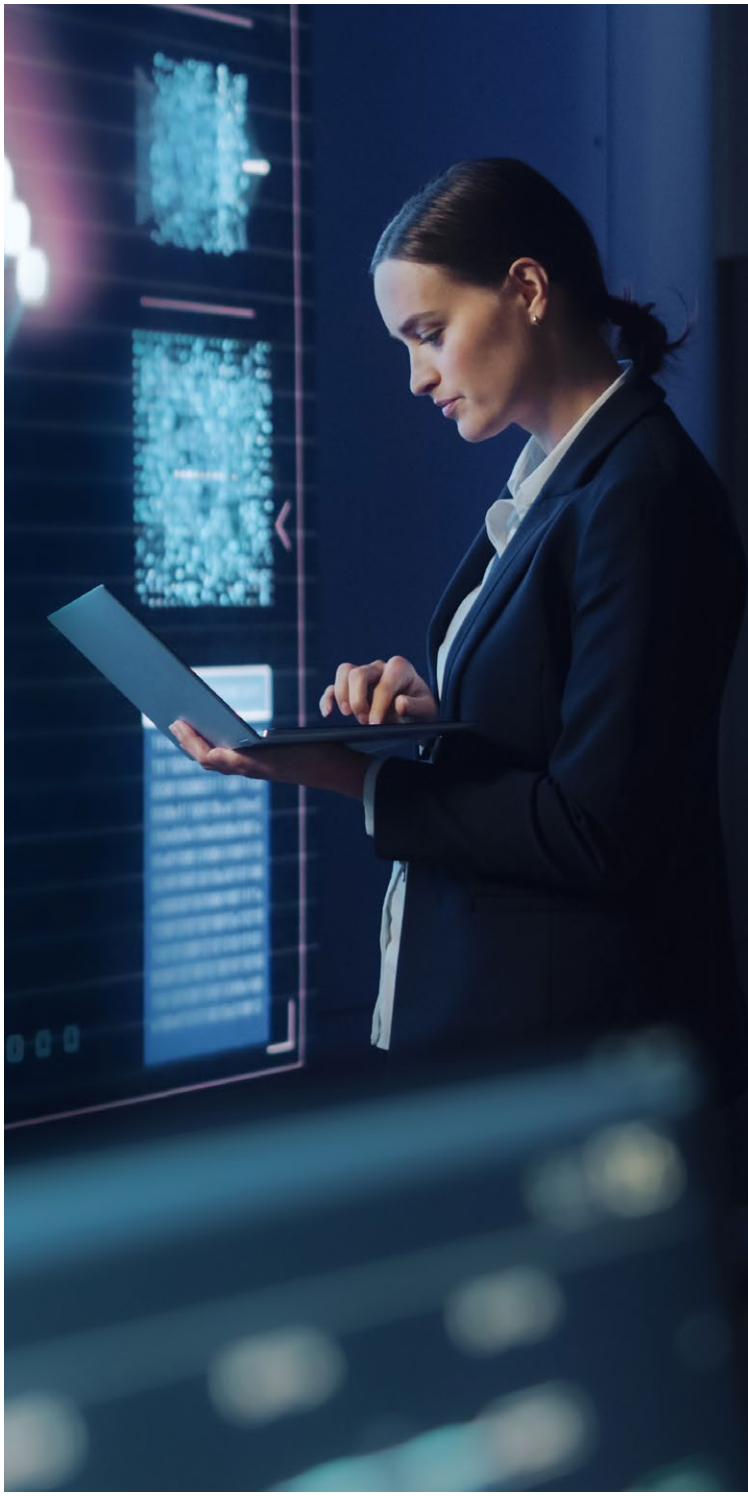
Cybersecurity efforts have demanded an increasing amount of the federal government's attention, and for good reason. Given that the government collects and stores large amounts of confidential data—including personnel, national security, and military data—it remains a prime target for cybercriminals. In addition to cyber threats from lone actors, the federal government also faces cyberattacks carried out by foreign governments—such as North Korea, Russia, and Iran. A few high-profile examples are the SolarWinds attack on federal agencies and the Microsoft Exchange zero-day attack that compromised more than 100,000 mail servers. As new types of technologies emerge, cyber-threat tactics and techniques must also be enhanced. Thus, it is imperative the federal government leverages best practices and obtains reliable solutions that will help protect against potential threats.



THE CRITICALITY OF FEDERAL CYBERSECURITY

The security of federal agencies' systems and data is vital to protecting individual privacy and national security. Risks to IT systems are increasing as more agencies shift information online and as cybercriminals become more willing and capable of carrying out cyberattacks. There has not only been an increase in the number of cyberattacks within the federal government but also an increase in the cost of recovering from these attacks.

To put it into perspective, each day the federal government fends off thousands of cyberattacks from adversaries.[1] A M-Trends 2023 report speaks to how the federal government is the number one target by a wide margin of 25% of attacks.[2] These attacks range from simple to more complex. For example, some of these attacks are simple phishing emails aimed at tricking a preoccupied federal employee, while others are more sophisticated and can target the nation's most precious data assets. In fiscal years 2021 and 2022, federal agencies reported 32,511 and 30,659 information security incidents respectively.[3]



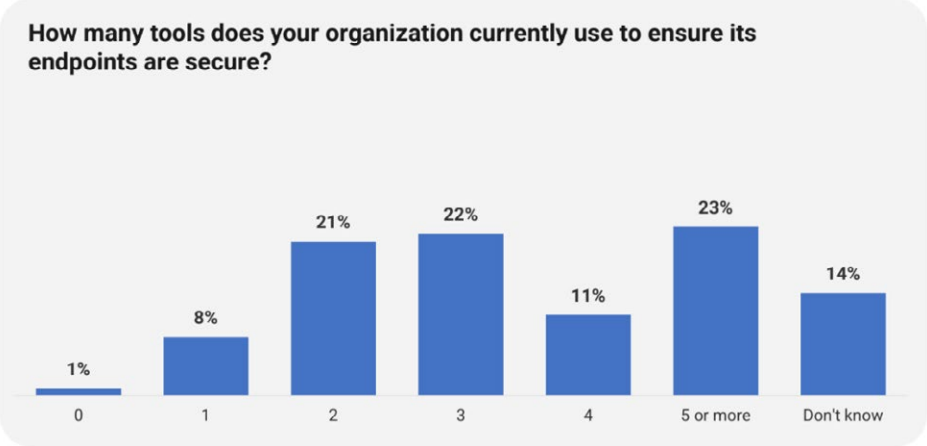
ENDPOINT SECURITY

Improving endpoint security is one key method of enhancing federal cybersecurity. Endpoints are physical devices that connect to a network—such as mobile devices, desktop computers, servers, and medical devices. These endpoints are vulnerable devices and popular doorways through which cybercriminals can exploit systems and steal information. Endpoint security safeguards these connected devices from malicious actors and exploits by examining files as they enter the network and addressing threats in real-time. Using an endpoint security solution allows agencies to monitor devices, and quickly detect malware and other common security threats before cybercriminals are able to attack.

In a 2023 Insights & Research Group survey, 70-79% of respondents disclosed that their agencies' top challenges regarding endpoint security are managing every workstation, server, and mobile device, as well as accessing known critical vulnerabilities in near real-time. Over half of the respondents said they are using three or more tools for endpoint security, and about 14% of all respondents were unaware of how many endpoint security tools their organization may be using.

Since the government is using more than one endpoint security application, it's likely they have far more operating systems than the endpoint security applications can handle. In order for endpoint security to be a reliable tool, it must be able to protect all of the endpoints an agency may have.

To aid in endpoint security and reduce the risk of cyberattacks against the government's digital infrastructure, the White House has instructed federal agencies to officially move towards a Zero-Trust approach to cybersecurity.[4] This cybersecurity approach eliminates implicit trust, denies access to digital resources by default, and grants authenticated users tailored access to only the applications, data, services, and systems they need to do their jobs.[5] The Continuous Diagnostics and Mitigation (CDM) Program has also been a dynamic approach in fortifying the cybersecurity of civilian government networks and systems by providing participating agencies with the cybersecurity tools, integration services, and dashboards needed to improve their respective security posture.[6]



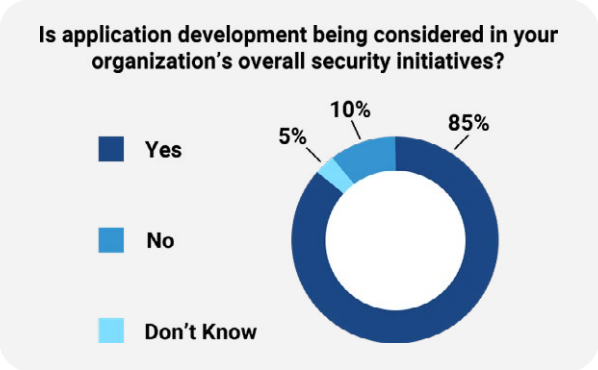
APPLICATION SECURITY TESTING

Application security (AppSec) is the process of using security software, hardware, techniques, and best practices to protect applications against external security threats. Proactive application security takes measures to predict and prevent an attack before it happens, fixing security gaps before they can be exploited and mitigating the highest risks to stay ahead of potential attackers. Application security testing (AST) is essential to proactively deterring cyber threats. AST pinpoints application vulnerabilities for quick remediation in every phase of the software development lifecycle. Some AST solutions are:

- **Dynamic Analysis Security Testing (DAST):** This solution tests applications and application programming interfaces (API) against potential vulnerabilities while applications are running.
- **Static Analysis Security Testing (SAST):** This solution analyzes source code in applications and API's for potential vulnerabilities earlier in the development process.
- **Interactive Analysis Security Testing (IAST):** This solution monitors applications and API's to help find and fix vulnerabilities without slowing down development.
- **Software Composition Analysis (SCA):** This solution identifies vulnerabilities introduced by open-source software components.

About 85% of government employees who participated in the 2023 Insights & Research Group survey disclosed that they are considering security initiatives because they are currently using training, awareness, and continuous monitoring to protect their application data. About 43% of respondents feel that they have integrated security tools for security processes, but could ultimately implement stronger practices. The majority of respondents (75-82%) feel that the top three application security challenges their agencies have are:

- Finding application vulnerabilities
- Lack of staff with the necessary expertise
- Remediating application vulnerabilities quickly



SOLUTIONS AND KEY CONSIDERATIONS

The U.S. Government Accountability Office (GAO) has made over 4,000 recommendations for federal agencies to address cybersecurity shortcomings. However, over 880 of these have not yet been fully implemented.[7] Until these issues are addressed, federal systems will be increasingly susceptible to cyber threats. GAO lists four cybersecurity challenges and ten critical actions to try and rectify the challenges over time:

1. Establishing a comprehensive cybersecurity strategy and performing effective oversight

- Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
- Mitigate global supply chain risks (e.g. Installation of malicious software or hardware).
- Address cybersecurity workforce management challenges.
- Ensure the security of emerging technologies (e.g. artificial intelligence and Internet of Things).

2. Securing federal systems and information

- Improve implementation of government-wide cybersecurity initiatives.
- Address weaknesses in federal agency information security programs.
- Enhance the federal response to cyber incidents.

3. Protecting cyber critical infrastructure

- Strengthen the federal role in protecting the cybersecurity of critical infrastructure.

4. Protecting privacy and sensitive data

- Improve federal efforts to protect privacy and sensitive data.
- Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Improved endpoint and application security are critical parts of the GAO's cybersecurity recommendations. These security considerations are vital to safeguarding the abundance of federal systems and information, as well as the nation's dispersed critical infrastructure.

President Biden's Executive Order on Improving the Nation's Cybersecurity (14028) also provides a mandate for agencies to improve cybersecurity efforts.[8] The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) published a set of DevSecOps best practices—"Securing the Software Supply Chain for Developers"— that provides cybersecurity guidance addressing high-priority threats to the nation's critical infrastructure.

The federal government does not have enough employees with the required cybersecurity skills which makes it nearly impossible for every agency to keep up with the copious amount of systems used and address the thousands of cyberattacks that are attempted daily. For this reason, the federal government must partner with the private sector to manage the immense need for endpoint and application security. These long-term public and private partnerships improve federal security and resilience. These partnerships benefit the federal government's digital environment by:

- Overseeing business processes
- Increasing information sharing
- Mitigating risk
- Innovating at the speed of the industry
- Leveraging industry expertise
- Reducing the need for trained personnel
- Improving overall cybersecurity performance

FINAL CONSIDERATIONS

It should surprise no one that cyber threats are here to stay. In fact, the latest developments in machine learning and artificial intelligence have only increased anticipated cybersecurity threats. It is imperative that federal agencies invest in reliable, fast-acting endpoint and application security tools. These tools, if managed correctly, can be a huge game changer in the amount and types of attacks that are able to pose a threat to our nation.

SOURCES

1. https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government
2. https://www.mandiant.com/company/press-releases/m-trends-2023
3. https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/#:~:text=In%20the%20fiscal%20year%202022,and%20non%2DCFO%20Act%20agencies
4. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
5. https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network
6. https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf
7. https://www.gao.gov/cybersecurity
8. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

A MESSAGE FROM OUR SPONSOR

HCLSoftware
Federal

As the federal government transforms its IT environment, it simultaneously is expanding its potential attack surface. Agencies need to build a best-in-class cybersecurity program that provides dynamic security and easier management – no matter the number of disparate tools or operating systems in place. This includes the ability to perform continuous monitoring, which can be challenging for federal agencies that manage multiple homegrown applications throughout their software development lifecycle.

HCLSoftware has long supported federal organizations on large initiatives such as the Continuing Diagnostics and Mitigation (CDM) program. It's a comprehensive solution for agencies and is aligned with the NIST 800-207 compliance standard. HCLSoftware solutions automatically and proactively build security into applications to achieve compliance and reduce vulnerability risks. Our technology uses machine learning to ensure that true potential risks are being presented, rather than false positives.

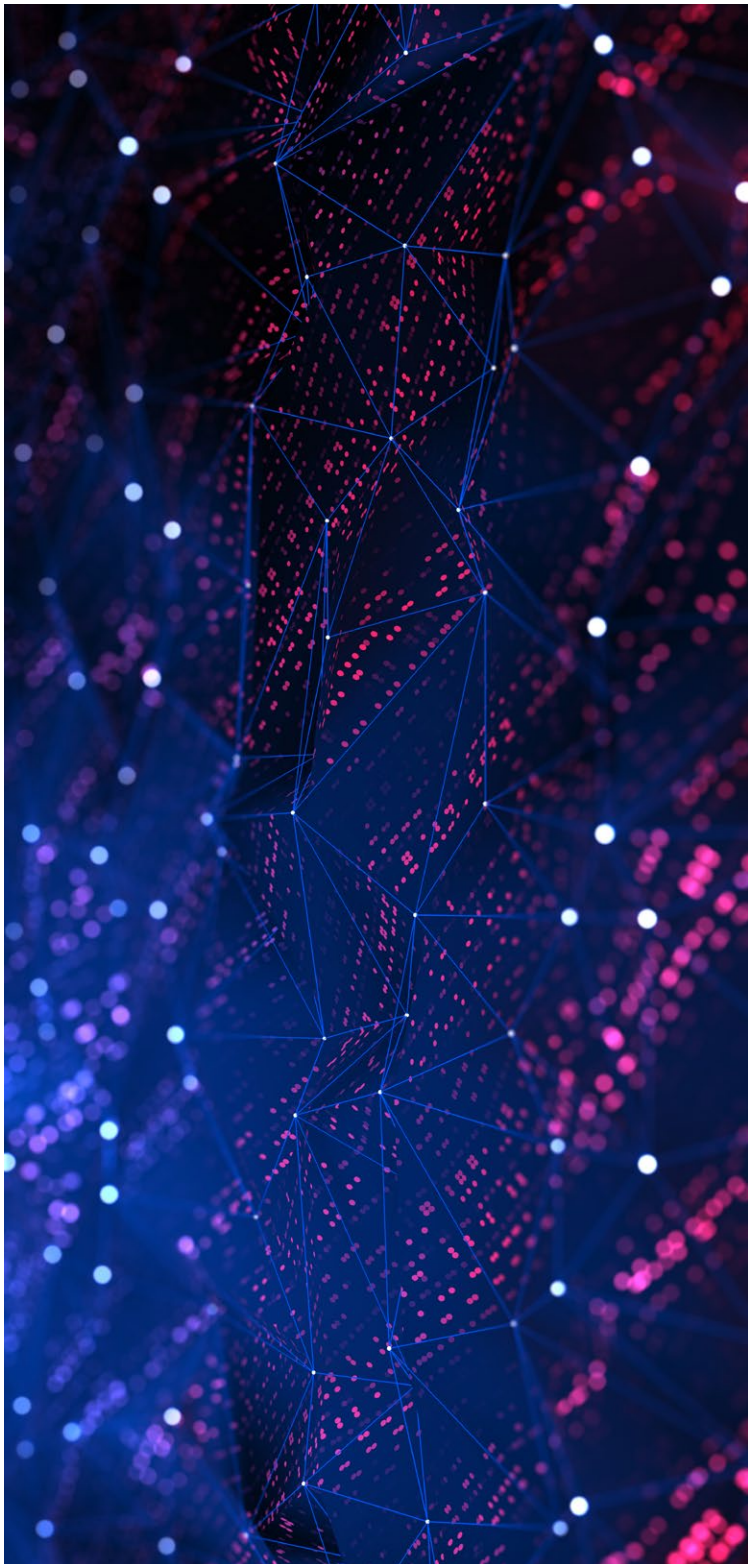
The right software partner understands the issues impacting government agencies and has the deep expertise and experience to address them. We are committed to helping government organizations meet not just today's threats and demands, but also whatever comes next.

ABOUT

Government Business Council

About GBC:

As GovExec'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 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis.



HCLSoftware
Federal

About HCLSoftware:

HCLSoftware is in a unique position to help government institutions digitally transform and provide citizen-centric digital experiences. Our products and services have been in use for decades, and have already transformed the IT environments of governments, both global and domestic. Furthermore, we constantly innovate and incorporate customer feedback to remain at the forefront of cybersecurity and digital transformation requirements.

Discover how HCLSoftware can help your agency modernize, satisfy performance mandates and transform to better address employee and citizen requirements.

Learn More at:
www.hclfederal.com