March 2022

AGA Research

The State of Cybersecurity in Government

AGA™

Acknowledgments

AGA is proud to recognize members of our Corporate Partner Advisory Group's (CPAG) Technology Committee for supporting this effort

Contributors

Team Lead: Andre Leroux, Senior Consultant, CGI

Denise Bottomley, Business & Technology Transformation Consulting, EY

Kerry Canfield, Vice President, CGI

James Cox, Manager, CLA

Stacy Dawn, Director Consulting Expert, CGI

Julie Edwards, Director, CohnReznick

Christine Horwege, Director, CGI

Kevin Greer, Vice President, CGI

Michael Huffman, Chief Growth Officer, cBEYONData

Jennie Melchior, Director, Guidehouse

Ryan O'Conor, Manager, CLA

Paresh Patel, VP Consulting Expert, CGI

Angela Rey, Technical Advisor

Bill Sterbinsky, Technical Director, CGI

AGA

Ann Ebberts, MS, PMP, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Mary Margaret Yodzis, Editor

AGA's Corporate Partner Advisory Group is a network of public accounting firms, major system integrators, IT companies, management consulting firms, financial services organizations, and education and training companies. These organizations all have long-term commitments to supporting the financial management community and choose to partner with and help AGA in its mission of advancing government accountability.

AGA is the association that provides a network for connecting and empowering financial and related professionals to **advance** good government, **grow** their expertise and **accelerate** their careers!

The State of Cybersecurity in Government

Table of Contents

Introduction

Since the early 2000s, discussions among agency executives on technology and digital transformation typically did not include cybersecurity funding requirements as a primary driver. Priorities changed over the last ten years as the technological capabilities of bad actors matured. Today, the increasing need for cybersecurity resources leads chief information officers (CIO), chief information security officers (CISO), Inspectors General (IG) and IT front-line leaders to examine and consider cybersecurity priorities with CFOs, risk and audit committees, and operational and program leaders. The growing reliance on technology and interconnections, intensified by remote work, demonstrates the urgency in every agency to prioritize technology to meet its mission.

Events in the past 18–24 months, such as the 2020 data breach in the federal government and the Colonial Pipeline ransomware attack, appear to have raised agencies' concerns about cyber risks in operations. To better understand the current costs and risks of cybersecurity, volunteers from the Technology Committee of AGA's Corporate Partner Advisory Group (CPAG) interviewed leaders from several agencies, including CIOs, CISOs and IGs, and reviewed related industry journals and government reports to assess present spending priorities, constraints, drivers and risks for federal agencies to meet their missions. AGA also gathered their recommendations for planning and managing cybersecurity budgets.

At AGA's Technology & Transformation Summit (TTS) in November 2021, a panel on "The State of Cybersecurity in Government" discussed ways agencies currently prioritize cybersecurity solutions for financial and technical management. Panelists shared their challenges in planning for, acquiring, implementing and monitoring new technologies, and they reviewed governmentwide and agency-specific policies and associated processes to meet the demands of an "emerging cyber pandemic." Session moderators also polled the audience of approximately 700 government and industry leaders on their top cybersecurity concerns. All polling data is included in this paper.

Executive Summary

The Technology Committee of AGA's Corporate Partner Advisory Group (CPAG) gathered information for this report through numerous interviews, peer-reviewed industry articles, and polls of government and industry leaders. The research aimed to elucidate difficulties in cybersecurity funding and present solutions to address ongoing resource constraints. Researchers also examined the impact of mounting business requirements and funding priorities to support cybersecurity.

Interviewees included leaders from four large agencies within the Cabinet of the United States who are responsible for risk reporting, mitigation plans, budgets and security posture. The research also delved into recent regulatory mandates and guidance on cyber activities, articles on the increasing cost of ransomware and cybersecurity measures, and the insights of practitioners who participated in a panel discussion on cybersecurity at AGA's Technology and Transformation Summit (TTS) in November 2021.

Four distinct themes emerged from AGA's research:

1. **Agencies struggle to acquire and preserve resources for cybersecurity.**

   The number of skilled professionals, the amount of technology funding, and the cybersecurity initiatives needed are not aligned with current business resource allocations. Near-term increases in funding and staff are not keeping up with the need for change and improvements, nor with required maintenance costs. Rapid technology advancement outpaced agencies' ability to hire, train and retain proficient cybersecurity personnel, mainly because the federal hiring process is slow and starting salaries are not competitive with more lucrative industry positions.

Which of the following events has created the most disruption to your short- and long-term funding plans?[1]

Choice	Percentage
A) Pandemic	52%
B) Employee turnover	26%
C) Regulatory changes	12%
D) Cyber threats or incidents (ransomware, attacks, forensics)	10%
E) Third party provider breaches	2%

Poll conducted at AGA's TTS 2021 on Nov. 18, 2021.

2 Crises affect priorities set by the agency funding model.

Agencies plan and allocate spending for long-term initiatives, complicating the appropriate apportionment or realignment of resources when a crisis occurs. Agencies not only need to respond quickly to threats and trends, but also need a proactive process to remain secure. Timelines for government contracts are elongated and burdensome, and they cause delays, constraints and inefficiencies in implementing upgrades and emerging technologies.

3 Technology and cybersecurity decisions need input from more than the CIO and CISO.

Most agencies view cybersecurity as a top priority. Yet lack of engagement at all levels of the organization exposes it to attacks and limits visibility for cyber leadership staff. Transformation efforts are most effective when product owners are committed at all operational levels.

4 Agency risk profiles are MODERATE with a trajectory to HIGH.

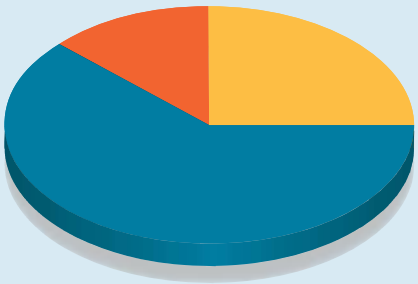
Cybersecurity is not a technical challenge; it is an enterprise risk management (ERM) challenge. Agency risk profiles are arguably "high" because federal entities are prime targets of cybercrime. The amount of data collected, transacted and stored by agencies is vast. Also, the compliance requirements for data governance and management increase an agency's risk profile. Nevertheless, attendees polled at AGA's 2021 TTS suggested current agency security posture may be moderate rather than high, as shown in **Figure 1**.

The remainder of this report details research findings, organized by the four themes stated above. It presents both cybersecurity challenges noted by agency leaders and recommendations for addressing them based on our analysis of the findings.

Figure 1. Agency Risk Rating

Based on the current security posture, compliance requirements and threats, how would you rate the risk profile at your organization or agency?

A) High 25%
B) Moderate 62%
C) Low 13%



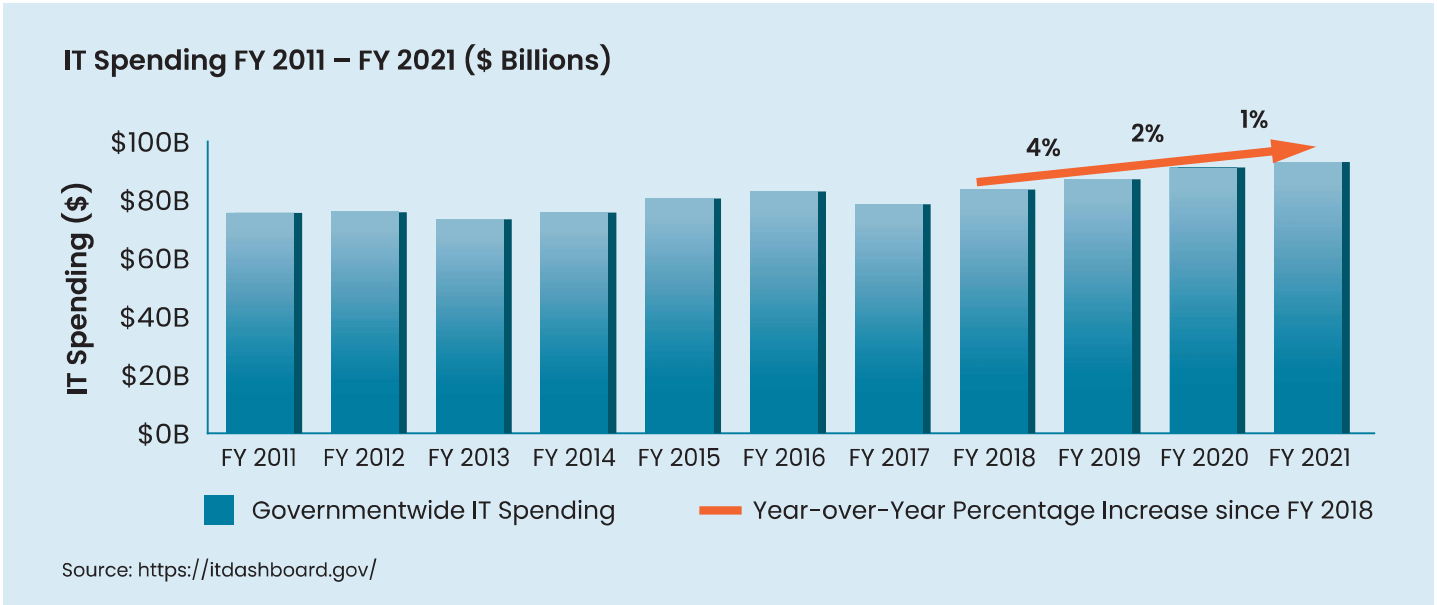
Agencies Struggle to Acquire and Preserve Resources for Cybersecurity

The uncertainty of available cybersecurity resources for the future directly affects an agency's ability to implement and maintain a comprehensive cybersecurity solution. Continued shortages in funding and personnel as well as complexities in managing technology are among the distinct concerns voiced by our interviewees. One solution is turning to trusted industry partners, an excellent resource for government entities seeking cybersecurity solutions.

Since agencies have trouble keeping up with rapid industry changes, and agency budgets usually require months to years of planning, getting outside help in cybersecurity may be necessary. Even with the transition to agile methodologies, federal budget cycles often do not align with needed technology and process updates, implementation deadlines or required reporting dates. Agencies must prepare to act quickly when a cyberattack occurs; the situation is urgent. More comprehensive IT strategic plans, plus action plans and roadmaps for transitioning from a current to a future state, can speed up agency response to critical threats.

Figure 2 illustrates governmentwide IT spending in the past decade and reflects a steady year-over-year increase since 2018, but this trend is not in line with agency automation and security requirements.[2] What the chart does not detail is that the increase in IT spending focuses primarily on health care agencies, Veterans Affairs, and the Department of Defense, leaving many other agencies' IT plans to stagnate or even decline. The more relevant measure is the percentage of spending on security and cybersecurity activities.

Figure 2. IT Dashboard Illustrates Agency IT Spending, Year-over-Year



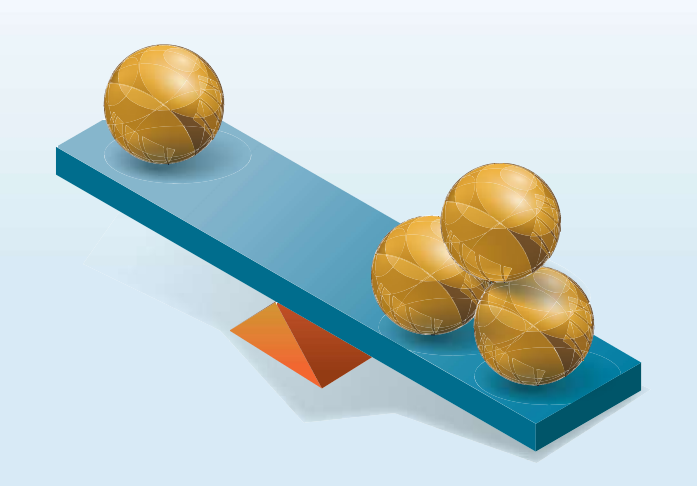
Source: https://itdashboard.gov/

Crises Affect Priorities Set by the Agency Funding Model

Agencies plan and allocate spending for long-term initiatives. Unplanned, short-term events can dramatically alter the availability of resources and strain an agency's funding capability to meet existing commitments alongside crisis response and federal mandates. As agencies struggle with these challenges, the supplemental appropriation will help them remediate pressing concerns, but it provides little to no resources to address future, unforeseen crises.

Risks are ever present, emergencies will undoubtedly occur, and agencies often acquire new responsibilities as top priorities while maintaining ongoing duties. For instance, COVID-19 forced agencies to create solutions and make large-scale changes in work environments to support ongoing operations during the pandemic, yet cybersecurity risks escalated with widespread telework. As more and more crises involve technology, the federal government may need to establish a Crisis Center of Excellence or Cybersecurity Center of Excellence involving collaboration among agency representatives to maintain operational progress as issues arise.

In preventative crisis management, the federal government struggles to meet the cost of technology implementation. Appropriating billions of dollars to remediate a hack like SolarWinds is simple in hindsight. Unfortunately, the initiatives that followed SolarWinds typically received little to no extra funding to modernize systems, despite mandates to upgrade. It is one thing to quantify cybersecurity risks, but another to complete business plans and align funding for them.



The latest cyberattacks on government agencies led to Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*. The EO and its complementary directives and memoranda instruct agencies to move faster to correct issues in the software supply chain, vulnerability reporting, information sharing, and compiled log data. While the EO is part of a broader cyber plan that requires the coordination of skilled personnel, technology and deployments, the prospect of accomplishing its goals is daunting. A common theme that emerged from AGA's interviews and research indicates that the expectation of agencies to respond to cybersecurity requirements far outweighs available resources — specifically, people, process, technology, time and budget.

Technology and Cybersecurity Decisions Need Input from More than the CIO and CISO

Discussions must move past traditional CIO and CISO initiatives to include agency business leaders so that agencies can fully grasp the challenges they face. These conversations are most often included in the ERM agency assessments and reviews. Almost every organization is dependent on technology. For many professionals outside the CIO or CISO offices, technology and cybersecurity are hard to measure and understand from a business perspective, because security is often counted as a preventative cost. Business metrics focus on growth, revenue and time to market, whereas cybersecurity metrics address loss prevention and potential costs, making business value comparisons difficult. As agencies become ever more dependent on technologies and networks for business operations, all executives need to understand the impact of security breaches and make more data-driven decisions related to security. Cybersecurity is not a technical challenge; it is a risk management challenge for the entire organization and should be highlighted in every agency's ERM planning.

Quantifying risk and assessing ways to mitigate risk helps leaders, like the agency head, chief management officer, Undersecretary for Management or CFO, understand potential problems. Management executives may not understand the technical aspects of a cybersecurity issue or potential threat, but they will understand impacts on operations. Therefore, they need to fully understand the "internal attributes of IT systems [that] create risks and opportunities and generate costs. These attributes determine just how agile and resilient an organization can be, as well as how productive each marginal dollar of IT spending can be."[3]

> Over the last few years, many federal agencies have lost highly skilled workers in a variety of mission critical areas, which has made it more difficult for the federal government to accomplish its mission. These workers include, among others, scientists, climate professionals, mine inspectors, civil rights attorneys, housing professionals, and personnel with acquisitions, human capital, and cybersecurity expertise.[4]

Agencies Need to Acquire and Retain Qualified Cybersecurity Personnel

Cybersecurity concerns have escalated from non-existent 20–30 years ago to a top-tier priority in many agencies. Rapid technological advancement has outpaced agencies' ability to hire, train and retain high quality cybersecurity professionals. The hiring process in the federal government is slow. Competent people may stay within the government system but often move on to other internal or external agency positions, stalling progress in the departmental initiatives they leave behind. Other considerations in this personnel predicament are attrition rates, not accounted for in staffing procedures, and siloed departments that prevent cross training within teams. Many managers struggle to see the long-term benefit in the short-term cost of cross training an employee in another department.

Several government agencies are allowed to use Direct Hire Authority to bring in cybersecurity and other needed skill sets faster. For example, the U.S. Department of Homeland Security initiated a Cyber Talent Management System to address challenges in hiring, compensation and career development and attracting quality cybersecurity personnel.[5] However, for most agencies, the General Schedule (GS) pay scale for federal employees is still not competitive with private sector salaries for cybersecurity personnel. The GS precludes agencies from extending competitive offers to potential cybersecurity hires by restricting position and salary levels to the number of years served in the federal government, not the number of years worked in cybersecurity in general. As a result, many agencies cannot compete in the marketplace for talent.

Instead of simple "pay comparisons," the federal government should spell out a total compensation package so that potential candidates can weigh salary plus benefits in their decisions about job offers. Job mobility is one benefit that the federal government should certainly highlight, given the offices in every (or nearly every) state in the U.S., as well as overseas. Government employees could potentially enjoy opportunities to move around to accept advancements, yet retain their benefits or tenure towards retirement by remaining with the federal government.

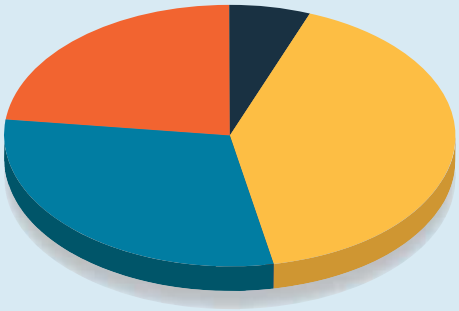
Endeavors such as the Office of Management and Budget's Federal Cyber Reskilling Academy attempted to train existing federal employees to meet upcoming cybersecurity demands. Although many attendees completed the required courses, they lacked the years of federal government experience to obtain positions that would qualify for higher pay as cybersecurity personnel.[6]

In addition, most cybersecurity personnel fall under the *2210 Computer Specialist* career field, a "catch all" for computer support that does not distinguish computer support by categories that compare with the IT industry. Some agencies encourage hiring managers to create positions in other career fields with fewer degree requirements; however, this approach could create problems because the overall requirements may eliminate cybersecurity positions. Business support functions, HR and the CFO staff, for instance, are not necessarily trained in or aware of the intricacies of cybersecurity, which results in incorrect job codification and funding. Agencies then find it even harder to compete for talent.

Presenting the threat, or risk, in a way that the business side of the agency comprehends will help the agency frame risks for informed decision-making about technology and cybersecurity issues. It must be made clear to financial leaders that the CIO and CISO need their help in addressing technology and cyber risks. Even though finance and operations departments may not understand the full extent of breaches or cyber incidents because of their technological complexity, they understand the funding requests to remediate damage, stabilize operations, and reinstate the integrity and availability of needed systems and data. Technology and security are no longer CIO-CISO problems; they are the problems of every leader in an agency.

There is a projected gap for security and technology skills over the next 10 years, what do you see as the primary constraint for acquiring your workforce needs?

- Industry is perceived more 'attractive' than government (pay, benefits, workplace, other) 41%
- Retention is difficult, causing turnover and loss of knowledge, skills and capability 30%
- Skillsets are constantly changing with the technology, tools, processes, cannot hire the right people fast enough 23%
- Pool of applicants does not meet requirements 6%



The Agency Risk Profiles Are MODERATE with a Trajectory to HIGH

Federal agencies are prime cyber targets because of their large amounts of collected, transacted and stored data. Recent reports[7,8] suggest a sound security posture and better compliance in the federal government, but a deeper dive into incidents, mitigations and current technologies indicate a different story. Gaps in software, services and supply chain risks have not been defined; plus, the size and scope of federal agencies cause mitigation efforts to take years to implement.

Cybersecurity is among the top three priorities in all federal agencies. An article in the *Summer 2021* issue of the *Journal of Government Financial Management* outlines the CFO's role in funding business initiatives and describes the significance of enterprise risk in prioritizing cybersecurity spending to protect taxpayers' money and information.[9] The article refers to business systems and ownership, rather than technology and security, as a responsibility that extends beyond the CIO and CISO. In our interviews for this report, a similar theme emerged. One agency leader said, "I really want to change the language... It is a mission and business system, and there is a business owner."

Since security systems directly influence the bottom line, their availability and capacity to store data, or their upkeep if they are legacy systems, influence operating costs, time to market, and customer delivery. One factor that affects federal agencies' cybersecurity management is the number of resources committed to compliance. Our interviewees openly shared information on the cost to meet system compliance requirements of the Federal Information Security Management Act (FISMA). In most agencies, the same personnel who keep data secure also must answer all of the compliance interviews and requests. Given time constraints and multiple demands in federal agencies, implementations can become rushed, incomplete or disjointed, leading to increased risk of attack and potential network security gaps. As agencies review the cost of compliance and business threats, limited resources remain to address emerging risks and apply complete changes to the business model. These impacts were evident as the COVID-19 pandemic rearranged priorities in many agencies. Therefore, agencies must view cybersecurity as a top priority in day-to-day operations and management and bring it to their technology status discussions.[10]

Recommendations

Some agency senior staff interviewed, as well as industry peer publications reviewed in this research, recommend that agencies:

- Revise their IT development approach and assign technology product ownership roles to business leaders.
- Update procurement processes to decrease time to market for new technologies.
- Improve communication within cybersecurity teams to enable cross training and support.
- Form partnerships with agency leadership to align and scale technology to meet operational, security and governance outcomes.

Summary

Our nation depends on every government agency making cybersecurity one of its top priorities for resource funding and risk reduction. Our polls provide evidence that cybersecurity is already a top priority; however, there is still more work to do to increase the participation and visibility of cybersecurity practitioners in the upper levels of business operations.

To achieve the desired result, the government C-Suite must become responsible for cybersecurity and technology decisions in tandem with operational decisions. If they have not already, agency leaders must shift their thinking about technology and cybersecurity strategies from the domain of CIOs and CISOs to a common concern of an entire agency. As the global community adjusts to the prevalence of complicated technology, connected devices, and competitiveness for limited cyber expertise, agencies, particularly the Office of Personnel Management, must become more agile in hiring, compensation and career development in the broader cybersecurity job market.

Based on your current business planning and funding process, how would you rank cybersecurity initiatives in relation to other funding requests for your organization or agency?

Choice	Percentage
A) Top 3	50%
B) Part of CIO budget planning only	28%
C) Not currently discussing	12%
D) Priority #1	10%

Poll conducted at AGA's TTS 2021 on Nov. 18, 2021.

> I really want to change the language...it is a mission and business system; and there is a business owner.
>
> —Jim Gfrerer

Endnotes

1 "The State of Cybersecurity in Government," Technology & Transformation Summit, Virtual Conference: AGA, T112, Nov. 18, 2021.

2 "Our information technology investments at work," https://itdashboard.gov/. Accessed Dec. 6, 2021.

3 Schwartz, M. "The CIO-CFO Conversation: Technical Debt—An Apt Term?" AWS Cloud Enterprise Strategy Blog, Dec. 16, 2020.

4 "Talent Surge: Playbook for Rebuilding the Federal Workforce," U.S. Office of Personnel Management, Dec. 2021.

5 https://www.dhs.gov/homeland-security-careers/cybersecurityservice. Accessed Nov. 11, 2021.

6 Bur, J. "What makes federal reskilling programs flourish or fail?" *Federal Times*, March 11, 2020.

7 Executive Office of the President of the U.S. *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018.

8 GAO. *High-Risk Series*: *Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP), March 6, 2019.

9 "The CFO on the Front Lines of Cybersecurity" *Journal of Government Financial Management*, Summer 2021, Vol. 70, No. 2, p. 26–30.

10 "2020 Global Security Attitude Survey," Crowdstrike.com.

AGA™

www.agacgfm.org