William Blair

Increasingly Sophisticated Threats and Evolving Workplaces Prompt Sweeping Upgrades to U.S. Digital Infrastructure

Extensive efforts to modernize and secure the U.S. government's digital infrastructure provide myriad opportunities for financial sponsors to invest in the government services space.

Industry Commentary

Josh Ollek
+1 704 969 1583
jollek@williamblair.com

Gordie Vap
+1 704 969 1581
gvap@williamblair.com

B.T. Remmert
+1 470 351 6927
bremmert@williamblair.com

Cooper Bradley
+1 704 969 1789
cbradley@williamblair.com

In May, malicious computer code attributed to hackers with ties to the Chinese Communist Party was detected in the U.S. telecommunications systems in Guam—the site of a U.S. military outpost critical to the defense of Taiwan and other American objectives in the Pacific. In 2022, Chinese hackers stole over $20 million in COVID-19 relief funds. In 2019 and early 2020, the Russian "SolarWinds" hack affected approximately 100 U.S. companies and government agencies.[1]

The United States' top global adversaries are becoming increasingly sophisticated and aggressive in efforts to steal intellectual property, personal information, and state secrets. They are also investing heavily in next-generation technologies to identify and exploit vulnerabilities in America's (often outmoded and outdated) digital infrastructure.

Simultaneously, a new paradigm is emerging for professionals in the U.S. The COVID-19 pandemic created a need for a federal workforce that can work remotely, accessing sensitive government data from a variety of locations and devices.

In the face of these challenges, the whole of government—including the Department of Defense, the intelligence community, and all federal civilian agencies—is engaged in a widespread effort to modernize the government's IT infrastructure and to establish its security and upkeep as indispensable to national security. This effort is a multi-layered sea change designed to fix longstanding problems. It significantly increases the size and accessibility of the addressable market for federal IT solutions and services, driving increased activity for financial sponsors who invest in the government services space and attracting new financial sponsors to the fold.

Considering the expanding market and growing investor base, we believe that now is the time to consider buying a platform or initiating a roll-up strategy in one of the multiple subsectors related to digital modernization and federal IT solutions and services.

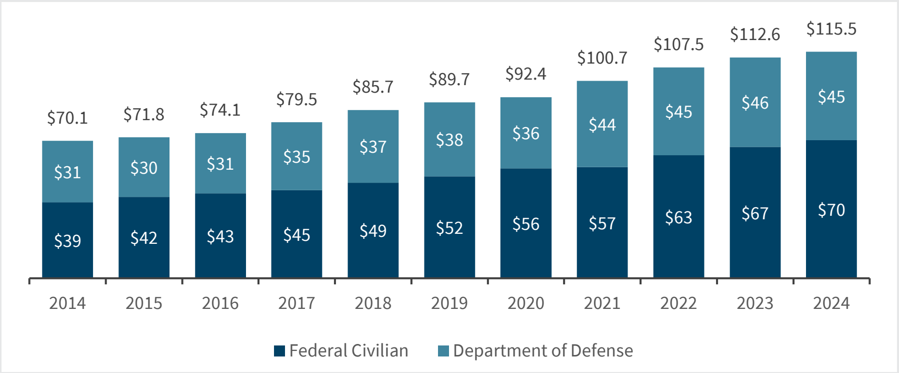
Revitalizing IT Infrastructure by the Numbers

As we look to 2024, the federal government is projected to spend over $115 billion on information technology for the Department of Defense, the intelligence community, and federal civilian agencies.[2] This commitment to increased spending bolsters other recent initiatives, including the creation of the Technology Modernization Fund, to facilitate technology modernization projects across the federal government. A report by the Government Accountability Office (GAO) published in May of 2023 highlighted the necessity of this investment. The report found that systems within the Department of Defense and Department of Homeland

1. Source: Center for Strategic & International Studies, Significant Cyber Incidents.
2. Sources: IT Dashboard, President Biden's 2024 Budget Request.

Large and Growing Government IT Budget[8]

($ in Billions)



Security had high vulnerabilities as a result of antiquated technology. These systems—which the GAO listed with only a numeric identifier because of their sensitivity—were over a decade out-of-date. Other critical federal systems are up to 15 versions behind the most current versions available in the commercial market, and some systems in federal civilian agencies are as much as 50+ years old.[3]

Additionally, the COVID-19 pandemic ushered in a structural shift in working dynamics that amplified the broader need for upgrades to the IT infrastructure. In a recent study, 95% of federal workers stated that despite the return to office, they retain the ability to work from home at least some of the time, and roughly a third of those who have left the government since 2021 cited a desire to work from home more frequently as their primary motivation.[4] This means that, in order to recruit and retain talent, the federal government must find and maintain ways for employees to access protected and secure networks from remote or hybrid work environments. Since a full two-thirds of federal agencies have not started or are still in the process of migrating data to cloud environments, significant funding and legislation are required to pursue these goals.[5] All told the sum of funding required to modernize the federal government's legacy systems could be upwards of $7 billion.[6]

Fortunately, lawmakers in D.C. have taken notice of the issue. Modernizing the federal IT infrastructure is one of the rare areas of the federal budget that receives bipartisan support. In June, for the second consecutive year, senators on both sides of the aisle introduced the Legacy IT Reduction Act, which aimed to force agencies to develop and implement modernization plans.[7] Furthermore, the federal IT budget has seen an uptick in annual funding from 4% annualized growth from 2013-2020 to 6% in the years since.[8]

Other countries, of course, face similar issues. Worldwide government IT spending is forecast to total $589.8 billion in 2023, an increase of 7.6% from 2022, according to Gartner®.[9]

Aligning with Federal Priorities

Financial sponsors considering the federal IT space have a bevy of possible entry points, including hardware, software, IT services, cloud services, and data analytics, along with opportunities emerging that can improve IT performance, efficiency, and security. Sponsors weighing their options should target companies aligned with the U.S. government's strategic IT priorities.

As outlined last year[10], those priorities are:

- **Cybersecurity:** Ensuring every department or agency is increasing the safety and security of its IT infrastructure, including reducing vulnerabilities by updating legacy systems (hardware and software). This includes creating secure, remote networks for intragovernmental communication as well as secure data access, storage, and transfer.
- **Increased Efficiency:** Adopting modern technologies and scaling them to make government run more effectively and efficiently. This includes the purchase of widely used commercial off-the-shelf solutions and operational technology (e.g., human resources systems, financial management systems, and cloud services) to meet the increasing speed of technological advancement.
- **Digital-First Customer Experience:** Using design and technology to deliver an exceptional customer experience for all end users that meets users' needs and is on par with modern customer expectations. This includes the design and implementation of networks to support mobile-first delivery of services.
- **Managing Data as a Strategic Asset:** Driving key insights into the decision-making process by harnessing accurate, available, and actionable data to power intelligent government operations and user experiences. This includes spending on commercial cloud computing, cloud-based software development, and data security tools, as well as efforts to leverage advanced analytics.

Valuation Considerations

Beyond alignment with government priorities, valuations for federal digital modernization businesses are driven by a number of factors, which are outlined in detail below.

Contract and Customer Access: Strategic and quasi-strategic (sponsor-backed) acquirers actively seek companies with specific contracts or access to specific customers to fill holes in their contract portfolios or expand strategically into new customer

[3] Source: U.S. Government Accountability Office, Testimony Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives, May 2023.
[4] Source: Federal Times, "Office reentry pushing feds to job hunt, Federal Times survey shows," Sept. 5, 2023.
[5] Source: Maximus & Market Connections, Maximus FedRAMP Survey Results Report, 2020.
[6] Source: Federal News Network, "The true price of technology debt," February 1, 2023.
[7] Source: Senator Hassan, "Senators Hassan and Cornyn Introduce Bipartisan Bill to Update Outdated Government IT Systems," June 15, 2023.
[8] Sources: IT Dashboard, President Biden's 2024 Budget Request.
[9] Source: Gartner Press Releases, Gartner Forecasts Worldwide Government IT Spending to Grow 8% in 2023, May 24, 2023. GARTNER is a regeistered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internatonlly and is used herein with permission. All rights reserved.
[10] Source: Federal IT Operating Plan.

sets. As a result, companies that have access to federal agencies or segments of those agencies with the largest and/or the fastest-growing budgets are highly attractive. Of course, long-term, stable contracts will draw more interest than short-term or research and development contracts.

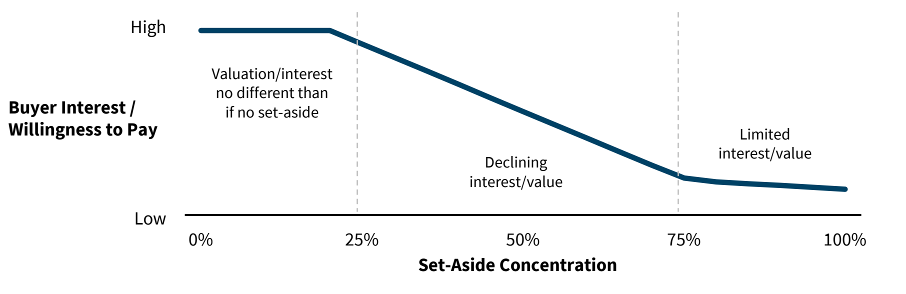
Differentiation of Offering: Companies with differentiated solutions and services are at less risk of displacement following a control sale, during a contract re-negotiation, or by competitors willing to compress margins to compete on price. Organizations with differentiated offerings often develop close relationships with agencies and contracting officers so that they can shape contract RFPs before they are published, increasing the odds of winning that opportunity as well as follow-on and adjacent opportunities. Businesses with highly differentiated capabilities can also more easily transition from set-aside contracts to prime, full and open contracts.

Business Model: Would-be acquirers highly value recurring revenue. While this is generally true across industries, it's particularly salient for companies that provide technology or tech-enabled services to government customers. Thus, providers of managed services are seen as more attractive because they generate more recurring revenue than providers of project-based services.

Reliance on 'Set-Aside' Programs: The portion of a company's revenue that comes from set-aside programs is another important factor. These programs award government work to organizations that qualify as small businesses, veteran- or minority-owned businesses, and other special designations. A company may or may not be able to maintain these designations or any of the associated contracts through a control sale, which is likely to give investors pause. Companies that rely on set-aside programs can mitigate valuation discounts by showing differentiated capabilities, strong relationships with customers and a track record of winning contracts in full and open competition.

Representative Valuation Impact of 'Set-Aside' Revenue[11]

Companies in the federal IT space are valued in part by how much revenue comes from 'set-aside' programs, which award government work to organizations with special designations (e.g., small businesses) that may be lost during a control sale.



Investing in the Future of Federal IT

As America's adversaries continue to advance technologically and remote work becomes a permanent fixture of American life, the need for sophisticated federal IT infrastructure will grow. At the same time, expanding federal initiatives, swelling funding, and cutting-edge domestic innovation are paving the way for strong opportunities in the federal IT space.

To learn more about opportunities in the federal IT infrastructure space, please do not hesitate to contact William Blair's aerospace, defense, and government services team.

This is the second article in our series on National Security Technology. In our previous article, we discussed how strategic acquirers are targeting companies earlier in their corporate lifecycle and how and why financial sponsors might consider adapting to the trend.

All statements in this report attributable to Gartner represent William Blair's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this report). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

"William Blair" is a trade name for William Blair & Company, L.L.C., William Blair Investment Management, LLC and William Blair International, Ltd. William Blair & Company, L.L.C. and William Blair Investment Management, LLC are each a Delaware company and regulated by the Securities and Exchange Commission. William Blair & Company, L.L.C. is also regulated by The Financial Industry Regulatory Authority and other principal exchanges. William Blair International, Ltd is authorized and regulated by the Financial Conduct Authority ("FCA") in the United Kingdom. William Blair only offers products and services where it is permitted to do so. Some of these products and services are only offered to persons or institutions situated in the United States and are not offered to persons or institutions outside the United States. This material has been approved for distribution in the United Kingdom by William Blair International, Ltd. Regulated by the Financial Conduct Authority (FCA), and is directed only at, and is only made available to, persons falling within COB 3.5 and 3.6 of the FCA Handbook (being "Eligible Counterparties" and Professional Clients). This Document is not to be distributed or passed on at any "Retail Clients." No persons other than persons to whom this document is directed should rely on it or its contents or use it as the basis to make an investment decision.

[11] Source: William Blair Research.