



BEYOND THE HYPE:

YOUR EMERGING
TECH PLAYBOOK

CONTENTS

3	Executive Summary
4	Data as Storytelling
5	Digital Citizen IDs
6	Cloud-based AI
7	Blockchain
9	Leading an RPA Revolution
10	Behavioral Biometrics
11	Augmented Reality
13	Open Source Accelerates AI Success
14	Bet Small, Win Big With Emerging Tech
17	Enabling Innovation through Privileged Access Management
18	States Embrace New Ways of Thinking
21	Cloud Provides Cost-Effective Solution to Data Backup, Recovery Challenges
22	8 Areas of Progress & Improvement in Government Technology
25	Mainframe Modernization: Paving the Way for New Possibilities
26	The Navy's Playbook for Playbooks
27	Emerging Technology Adoption: Questions to Consider
28	What's Next?
29	About & Acknowledgments

EXECUTIVE SUMMARY

In the not too distant past, the phrase “emerging technology” had a futuristic sound, alluding to technology that might make a difference in government operations...someday...maybe. That is no longer the case. In this era of continuous development, agencies are looking to understand, test and adopt emerging technologies quickly – and to begin reaping the benefits.

That is why the Department of the Navy (DON), in February 2019, announced the creation of NavalX. The organization is focused on identifying “isolated pockets of excellence” in innovation and scaling them out across the department – in the same vein as the Defense Innovation Unit at the Defense Department (DoD).

Across DoD, organizations want to accelerate their adoption of commercial technology innovations, rather than develop DoD-specific solutions, said Kevin Burnett, Pioneer in Residence at NavalX.

“In a lot of areas within DoD there’s now an acknowledgment that we can leverage the work that industry has already done and apply it to our DoD use cases,” Burnett said.

Look for Burnett’s advice on how to use the playbook concept to ease the adoption of emerging technology on p. 26.

State agencies also are increasingly interested in technology innovations, according to the latest annual survey of state chief information officers (CIOs) by the National Association of State CIOs (NASCIO) and Accenture. “Innovation and Transformation through Technology” made its first appearance on the top 10 list of technology and policy priorities, according to the report.

Meredith Ward, Director of Policy and Research at NASCIO, attributed the rising interest to a convergence of factors, including increased public demand for online citizen services at a time when many state workforces are shrinking and budgets remain constrained.

In our Q&A with Ward, which begins on p. 18, she also discusses the challenge of cultural resistance within agencies.

Culture is a recurring theme whenever IT leaders talk about emerging technology. It’s not only that agencies need to mitigate cultural resistance; they also need to cultivate behaviors that support innovation. During a recent GovLoop Virtual Summit, Craig Fischer, a Program Manager in the Office of Financial Innovation and Transformation (FIT) at the Treasury Department’s Bureau of the Fiscal Service, talked about the value of a “scanning culture” in which people constantly track new ideas being adopted in other agencies and the private sector.

Read about that and other best practices Fischer shared on p. 23.

The emerging technologies themselves are the heart of this guide. We chose to spotlight six that appear ready to move from the experimental/pilot stage into operations. Keep in mind that “emerging” does not mean “new”; a technology can be around for a long time (e.g., behavioral biometrics) before making that leap into full deployment.

Check out the full coverage, beginning on p. 4.

DATA AS STORYTELLING

In 1900, W.E.B. DuBois curated a meticulous data exhibit in Paris on the state of black life in the United States. He called it “an honest, straightforward exhibit of a small nation of people, picturing their life and development without apology or gloss.”

The data visualizations, derived from census data and Bureau of Labor Statistics reports, displayed statistics on black property ownership and population growth as more than numbers and colors. They told the data story of black Americans’ progress at the turn of the century.

The exhibit distills what data storytelling is and why it matters. Data storytelling uses visualizations, narratives and context to engage people with data and to help them think critically about it and the issues at hand.

For government, data has never been in a more prominent position. The Foundations for Evidence-Based Policymaking Act of 2018 calls for data-backed evidence to inform policymaking, and the Federal Data Strategy likewise fuels practical steps to use data strategically. Presenting data in a compelling way, through telling stories, can cut through the noise in a data-inundated environment and engage with stakeholders meaningfully.

CASE STUDY

With the collaboration of several local departments in San Francisco, the city released a beta site called the San Francisco Housing Data Hub. The web portal provides residents with data on housing in a storytelling approach.

Instead of dropping datasets into its open data website, datasf.org, the city organized an online hub to visualize and provide context on housing data for residents. For example, the website provides an overview story on the state of housing so that site visitors can better understand the programs and policies the city enacts.

The overview checks off data storytelling’s three elements. It visualizes its data by presenting interactive graphs, and it weaves narratives into them by cohesively linking the graphs. It directly takes into account the context of such data by addressing elements that residents — and potential residents — care about, such as population, renter/owner ratios and affordability.

BEST PRACTICES

To use data storytelling best, follow these steps.

- 1. Remember the three key elements to data storytelling:** Visualization, narrative and context.
- 2. Begin with a question about your goal and your audience.** Asking questions is the first step to strategically approaching data. It’s the same when it comes to using data as storytelling. First, decide what you would like to accomplish or what kind of impact you would like to have. Then, gauge your audience so you can most effectively achieve that goal.
- 3. All storytellers are biased, so acknowledging and mitigating potential bias is crucial.** Data’s objectivity may seem like it makes data storytelling inherently more objective, but the truth is all narratives are subjective. Account for this bias by fostering critical thinking and engagement with data stories. It leads to better-informed decisions in the end.



DIGITAL CITIZEN IDs

Governments provide a host of convenient digital outlets for citizens to access government services, such as filing taxes, enrolling for health care coverage or applying for citizenship. But users usually have to create a new digital identity for every service they need to access. This leads to a cluttered, inconvenient experience for users, who need to keep track of their separate logins.

As digital services in government have expanded and innovated, the access points through which citizens can use these services need to keep pace. If agencies across state, local and federal spheres are serious about delivering better digital services, a unified digital citizen identity is necessary.

So far, agencies have made strides in strengthening internal-facing identity and access management systems, such as Login.gov. But with the expansion of and commitment to public-facing digital services, providing a convenient, secure digital citizen identity is important to ensuring a seamless experience for critical services.

CASE STUDY

Utah first started working on its single sign-on (SSO) capabilities internally, enabling employees to gain seamless access to the applications they need. Called Utah-ID, the initiative provides access to about 900 applications and services.

In 2016, the state kick-started a public-facing SSO system by creating a business portal. The portal allows anyone doing business in Utah to access state-collected data relevant to their business operations, including business registration, workers' compensation and tax liability. Through the system, businesses can make payments, see a list of state requirements for operation and review completed items.

The business portal is the first step to providing SSO for the larger Utah public. Urged by legislators, the Department of Technology Services is working to integrate Medicaid agency applications into SSO, so it helps a larger swath of citizens who access services across the health and human services departments.

BEST PRACTICES

With these practices in mind, it is possible to attain modern digital citizen identities with government-grade security.

- 1. Establish the right governance model.** This means choosing the best identification and authentication process, most likely with the help of third-party digital identity service providers. According to Gartner, at least 80% of government services that require authentication will use multiple such providers by 2023.
- 2. Rethink identity design with tiered security.** Prioritizing security in identity management hasn't always led to a convenient or pleasant user experience. To not compromise on either, establish tiered security measures that depend on a specific service. For example, security can be less rigid for users booking an appointment at a facility vs. filling out a census form online.
- 3. Step away from knowledge-based verification,** as the National Institute of Standards and Technology (NIST) urges. This method assumes that only the authentic user would know certain identifiable information – thus, “knowledge-based” – such as birthdate and address. Instead, the Government Accountability Office (GAO) recommends alternatives such as mobile two-factor authentication.



CLOUD-BASED AI

The intersection of cloud computing and artificial intelligence (AI) is gaining attraction in the public sector.

AI involves machines imitating human cognitive abilities such as learning. Cloud, meanwhile, virtualizes access to computer system resources, such as data storage. Individually, each technology has proven its value. Together, AI and cloud can become a powerful duo for agencies at every level.

Cloud's flexibility means it can scale to fit any amount of data. This data fuels AI to make informed decisions, automate manual tasks and assist humans. Ultimately, cloud-based AI can help deliver public services smarter and faster.

AI could transform government responsibilities such as financial and military operations on its own, but cloud is a force multiplier that can drastically scale up its abilities. Cloud can exponentially improve AI because the flexibility it offers allows agencies to handle increasingly large amounts of data.

When paired, AI and cloud could dramatically change the way agencies operate. Naturally, getting the mix right is one of society's biggest concerns.

CASE STUDY

DoD sees cloud-based AI as the key to making the most of the U.S. military's mountains of data.

Lt. Gen. John N.T. "Jack" Shanahan, Director of DoD's Joint Artificial Intelligence Center, said that only an enterprisewide cloud can support AI for all of America's armed forces. "That's the lodestar," he said at the Armed Forces Communications and Electronics Association's AI and Machine Learning Summit in March 2019. "Without that, it's just sidecars and side projects."

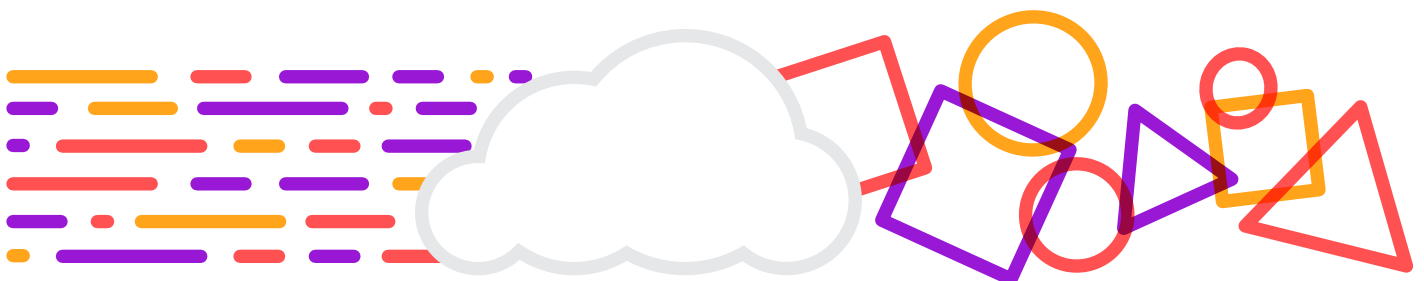
Shanahan added that AI needs enterprise cloud to handle DoD's data in real time and assist warfighters' missions. Although DoD had 400 to 500 AI projects in March 2019, he still saw enterprisewide cloud as the cornerstone of its AI efforts going forward.

"It's about what the entire U.S. society needs to do to stay ahead with its competitive advantage," he said of cloud-based AI's potential impact on America's military.

BEST PRACTICES

Cloud has long been a prominent subject among agencies at every level. AI's potential, meanwhile, means its buzz is quickly catching up to the interest in cloud. Here are some of the best practices GovLoop has encountered for fusing both tools:

- 1. Make sure the workforce is part of the plan.** As agencies adopt cloud-based AI, they need to ensure that existing employees – not just the technology experts but the mission experts, too – have the skills they need to support these initiatives.
- 2. Prepare to compete for talent.** The same concerns will loom large as agencies recruit new employees. And here's the catch: The competition for AI, cloud and data talent is fierce.
- 3. Deal with technology debt.** Legacy systems cannot store, process or transfer large amounts of data quickly enough for useful AI. Cloud can address this issue by modernizing IT so that it's agile and scalable enough for AI's complicated processes.



BLOCKCHAIN

Blockchain has the potential to transform the accuracy and security of government records.

Although its potential isn't fully realized yet, blockchain is promising because it provides an automated system for ensuring that the data in a digital transaction cannot be changed or deleted. Editing blockchain records requires complex mathematics, so altering the information they store without permission is incredibly challenging. What's more, users can see changes to their blockchain records, ensuring that no one tampers with them. For this reason, many supporters claim blockchain is secure by design.

The possibility of accurate, secure and transparent recordkeeping has made governments at every level increasingly interested in blockchain, which some are testing with pilot programs. These experiments may lead to blockchain initiatives that keep records about subjects such as crime, finance and homelessness.

Ultimately, blockchain's resistance to data modification could make it ideal for safely storing data long-term. Although blockchain hasn't passed the test of time, it's a technology that's a hot topic with federal agencies right now.

CASE STUDY

Rhode Island's interest in blockchain demonstrates the technology's versatility.

In May 2019, the state issued a request for proposals (RFP) from blockchain companies in areas where blockchain might improve efficiency and transparency, such as antifraud, contracting and medical marijuana.

The state also suggested that the technology could meet several needs in the same field. First, the recent RFP called for projects demonstrating blockchain's ability to reduce potential fraud and abuse in the medical marijuana industry. According to the RFP, blockchain would theoretically accomplish this outcome "from seed to sale" by keeping more accurate, transparent records.

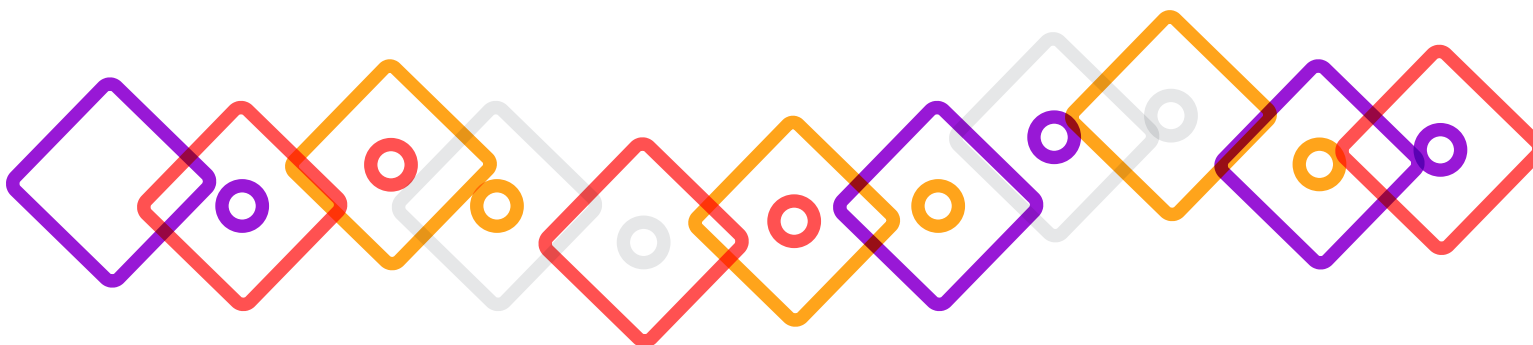
Additionally, the RFP requests evidence that blockchain could help craft authoritative records detailing the chain of custody for criminal investigative evidence, including medical marijuana probes and prosecutions.

Blockchain's adaptability raises the bar on how many solutions it might offer agencies.

BEST PRACTICES

Government engagement with blockchain is growing, so discussions about how to best implement it are also on the rise. Here are some of the strongest best practices around adopting this tool:

- 1. Start with good data.** Blockchain is only as valuable as the data it protects. Before you launch a blockchain initiative, ensure that the data involved is clean and accurate.
- 2. Go with experience.** Yes, blockchain is an emerging technology in government, but it has been put to use in other industries, notably the financial sector. In undertaking blockchain initiatives, lean on the expertise of industry partners with proven track records.
- 3. Don't rely wholly on blockchain for security.** Although blockchain helps secure data, agencies should still practice strong cyber hygiene. Agencies that educate their employees about cybersecurity are less likely to have mishaps with or without blockchain.



MEET THE NEW DIGITAL WORKER

LEARN MORE



LEADING AN RPA REVOLUTION

An interview with Keith Nelson, Global Head of Public Sector,
Automation Anywhere

A single robotic process automation (RPA) bot can save agencies thousands of full-time employee hours every year. Multiply that across more than 100 bots, and then RPA's full potential is realized.

Still, when learning about the benefits of RPA, organizations frequently focus on single case studies of how one bot alleviated the repetitive, manual workload of one task. Of course, these stories are important to anecdotally illustrate how RPA works, but isolated instances fail to capture the scope of transformation that RPA can have on an agency.

"This is a technology that can actually help drive the bottom-line benefits, the mission of what government's intended to deliver," said Keith Nelson, Global Head of Public Sector at Automation Anywhere, a company that offers easy-to-build RPA solutions for government and the private sector.

GovLoop recently spoke with Nelson about how to make the most of RPA at agencies. It turns out, many are missing out on RPA's full potential because their scope is too limited.

With bots, Nelson said, there is strength in numbers. Therefore, an agency will really unshackle employees and promote innovation by deploying automation enterprisewide. Four or five bots aren't enough for an RPA revolution; dozens or hundreds of bots are needed, Nelson said.

Several common pitfalls have organizations spinning their wheels on RPA transformation projects, however. Agencies can be decentralized in their approach, for one, leading to duplicative, labor-intensive and piecemeal developments. Also, agencies can fail to pair business needs with bot development, leaving important opportunities unfilled and IT teams unprepared.

Both of these trip-ups are resolved by a formal, organizational strategy for RPA. Although RPA pilots should start small – a common truism for technology projects – agencies should have an end state in mind and a plan to get there from the get-go. A central office for RPA will help to suffuse its adoption throughout an agency.

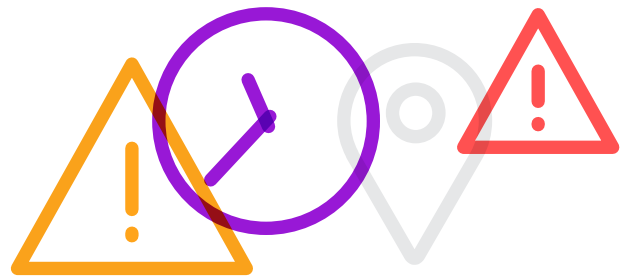
Of course, plans are often easier said than done, which is why agencies need to find tools that can easily link business needs to RPA development. Better yet, everyday users should have the opportunity to build the bots themselves.

"You really can't scale if every time you want to build a bot you have to wait in line for IT to get back to you," Nelson said.

Automation Anywhere offers an easy-to-use suite of capabilities that oversees all bots in production or in use. Users can simply hit "record" on Automation Anywhere's app, perform the manual task, and the RPA bot will copy and remember those actions for reuse. The tool is easy enough for business users to design bots and nuanced enough for developers to integrate AI into more complex models, meaning that with Automation Anywhere, agencies can thoroughly scale. Like spokes on a bike wheel, successful bots radiate from a central hub – and work together. And with the wheels of an RPA strategy in motion, agencies can cover a lot of ground.

Takeaway: *Automation was never about just one or two processes being streamlined. Bringing in user-friendly platforms, agencies can scale automation throughout their enterprise – led by everyday users who, with no-code and low-code solutions, build bots to answer business needs.*

BEHAVIORAL BIOMETRICS



The definition of biometrics can be inferred from the name – measures of unique biological or physical characteristics. Biometrics are often used to identify individuals based on their unique attributes, such as fingerprints, irises or DNA.

The U.S. government has been a leader in biometrics, with NIST constructing a global system for fingerprint recognition and the Homeland Security Department's Office of Biometric Identity Management containing more than 200 million unique identifiers.

Biometrics are often used to authenticate somebody's identity, such as a fingerprint scanner or facial recognition on a cell phone. However, as singular as these checks are, modern cybersecurity demands another level of verification as deepfakes and hackers threaten traditional forms of authorization.

Behavioral biometrics apply the same principle of unique identifiers to an individual's behavior. Instead of fingerprints and faces, they track keystrokes, geography and screen usage, all of which are patterns of a digital user. What's more, behavioral biometrics can shut down a hack even if the intruder has all of the right information.

As the government increasingly targets perimeter-based security and continuous checks of access and authorization, behavioral biometrics represent a resolute new means to keeping agencies safe.

CASE STUDY

Behavioral biometrics have many applications, all tracing back to security. From voice recognition to digital signatures to keystrokes, behavioral biometrics are in play to keep accounts secure.

The International Biometrics + Identity Association defines four applications of behavioral biometrics: continuous authentication, risk-based authentication, insider threat detection, and fraud detection and protection.

For one example, NIST is working on standards for voice recognition, which analyzes a speaker's voice for signature features, such as tone and pace, not to decipher words, as in speech recognition. NIST's work to standardize the physical biometric of fingerprints has allowed governments to share information and establish consistent user profiles, and voice recognition has similar potential.

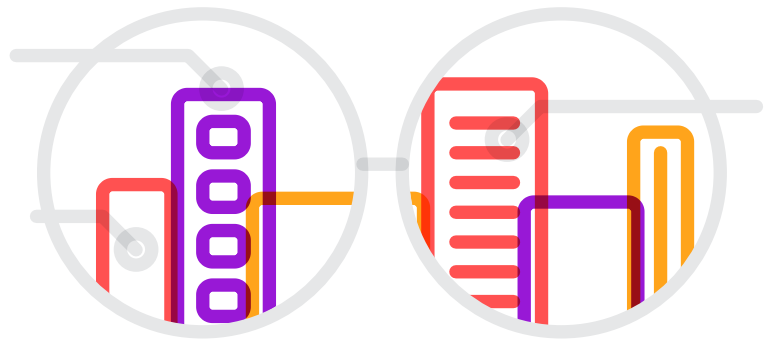
Elsewhere, the Defense Advanced Research Projects Agency has studied active authentication, providing continuous verification of a user's identification in addition to a single password gateway. By examining how the user maneuvers the mouse or crafts language, supervisors could raise a red flag to suspicious behavior.

BEST PRACTICES

The best practices associated with behavioral biometrics are similar to those associated with most new cyber solutions.

- 1. Ensure nuance.** Behavioral biometrics are a complex field, and the system therefore can't be subject to small sample sizes or user error. If an individual logs in once at an odd hour, that doesn't mean they're stealing information.
- 2. Put the infrastructure in place.** Behavioral biometrics require both a baseline profile and ongoing analysis. Some sort of technology, whether machine learning or smart sensors, is needed to build and analyze vast profile datasets.
- 3. Decide what level of risk you want to accept.** Behavioral biometrics are not a one-size-fits-all solution. Some users might not have access to sensitive data, so their profiles can be afforded slightly more risk.
- 4. Prioritize productivity.** If organizations are too restrictive, false positives can shut users out of their accounts and stall productivity. False positives could be triggered if a user is in a different country than usual or tries to log in from too many devices.

AUGMENTED REALITY



Augmented reality (AR) is getting real.

AR is an integrated platform that layers computer-generated sensory information on top of a real-world environment. The most common AR environments reflect the physical environment around the user while incorporating visual digital elements. Many also tie in audio and other perceptual inputs.

The first breakthroughs in AR came in the early 1990s from the government – specifically, the Air Force. The description provided in a 1992 report is still pertinent today.

“Tools and fixtures in the real world (e.g., a ruler guiding a pencil) enhance human performance by guiding manual operations, providing localizing references, reducing mental workload, and increasing precision,” the report states. “Virtual fixtures are computer-generated percepts overlaid on top of the reflection of a remote workspace which can provide similar benefits.”

But AR’s power and popularity have grown recently because of wireless technology and high-speed networks. Whereas original AR systems were cumbersome and wire-based, mobile devices can now access wireless networks or small computing chips for greater power and speed.

CASE STUDY

One benefit of AR is that it can simulate and enhance real-world scenarios when they are dangerous, inaccessible or expensive to recreate. For the Army, preparing soldiers for the battlefield remains one of its most important – yet also most expensive and difficult – responsibilities, as reflected by its budget.

In 2019, the Army teased a new visual “heads-up” eyewear, the Integrated Visual Augmentation System (IVAS), which will provide a unified platform of training and preparation for soldiers. IVAS is portable and easily wearable, attached by a headband with goggles and additional hardware worn on the back of the head.

The technology integrates 3D mapping, thermal imaging and training tools into real-world environments, allowing for realistic combat training in a variety of contexts and situations. IVAS will improve soldiers’ situational awareness and lethality for missions, officials said.

“This is cutting-edge technology,” Gen. James McConville, Army Chief of Staff, told the House Armed Services Committee’s Readiness Subcommittee in May 2019. “It is going to transform the way we train soldiers and the way soldiers operate in combat. We’re excited about it.”

BEST PRACTICES

Agencies are still learning AR best practices, but here are some of the emerging lessons.

- 1. Know where your organization stands with tech.** If your organization is restrictive about apps or personal devices, AR might fail to get off the ground or be widely accessible.
- 2. Know your physical environment.** The physical environment provides more limitations and opportunities that developers need to consider. Think about if the device has to be level-set, its view unobstructed or its surroundings carefully controlled.
- 3. Remember the purpose.** Ask yourself what AR provides that a handbook or demo could not. Hands-on trainings, such as preparations for surgeries or operating a piece of equipment, are great examples.
- 4. Engage the users, but don’t overwhelm them.** You can include all types of layovers, but don’t lose the reality in the process. Be sure that the virtual additions are meaningful, but make them simple and intuitive.



Red Hat

Enabling Your Public Sector AI

- Article: [The Democratization of Artificial Intelligence \(and Machine Learning\)](#)
- Webinar: [Accelerate Artificial Intelligence and Machine Learning in the Cloud](#)
- Open Source Stories: [AI Revolutionaries](#)
- OpenShift: [AI/ML on OpenShift](#)



OPEN SOURCE ACCELERATES AI SUCCESS

An interview with Chris Sexsmith, Cloud and AI/ML Field Strategy
Lead for the Public Sector, Red Hat

For government agencies, AI has the potential to be transformative, providing an unprecedented leap in the ability to manage operations, deliver services and support the mission. But like any new technology, AI requires the right platform. In particular, agencies need to ensure that they don't lock themselves into a proprietary platform that puts unnecessary constraints on their initiatives.

That is why open source is critical to the future of AI and ML. To learn more about the intersection of open source and AI, we spoke with Chris Sexsmith, Cloud and AI/ML Field Strategy Lead for the Public Sector at Red Hat, an open source software solutions provider. He talked about three primary benefits of deploying AI on an open source platform.

1. Increasing the transparency of AI

Open source helps remove the opacity from AI, Sexsmith said. This is important because as data science progresses, data and code become increasingly entangled. That makes it very difficult to understand how an AI system reached a given conclusion – in which case, people are less likely to trust the output. A proprietary platform only exacerbates the problem, Sexsmith said.

"Proprietary code might execute the task marvelously, but when it comes to auditing that entire process, it becomes much more difficult to explain how it came to the conclusion that it came to," he said. "If you can't see the code, it becomes more difficult to explain the system as a whole."

2. Democratizing AI

One reason AI is coming of age now is that the underlying technology is there to support it. The industry is at a technological maturity level that allows accelerators such as graphics processing units (GPUs) to be made accessible to all without breaking the bank, Sexsmith said.

"Openshift, via Kubernetes, enables GPUs to be distributed at a granular level to AI/ML workloads and consumed by teams in an as-a-Service model," he said. "Optimizing these limited resources allows existing data science teams to do more with less, thereby freeing up budget to do more data science."

By spending money on data science, rather than the underlying technology, agencies can put the technology in the hands of more data scientists and extend AI's reach.

3. Extending the DevOps mindset to data, ML

DevOps changed software by bringing together the development and operations teams to work together in a consistent, shared framework. But it's even more important to add data to the mix, Sexsmith said.

"Code itself doesn't do much with data, so it's critical for us to think of data/code entanglement as a living, breathing organism," he said. "If the data is old or incomplete, or if we don't fully understand what that data signifies, even the best code in the world will yield meaningless results."

From its earliest days, open source software has served as a platform not just for technology but for a culture of collaboration. That culture will be vital to the development of AI, Sexsmith said.

BET SMALL, WIN BIG WITH EMERGING TECH

José Arrieta is wired differently.

The Health and Human Services Department Chief Information Officer has made a career out of placing small bets in the government technology and acquisition spaces. These calculated risks have evolved over time. They've opened the door for multimillion-dollar savings and are poised to change the way some 3,000 acquisition professionals at HHS use data and technology to make more informed buying decisions.

A little over a year has passed since he first came to HHS. Recently, Arrieta spoke with GovLoop about how he has used his strengths to take managed risks and how he has tried to create an experience for employees so they want to use new tools and work differently.

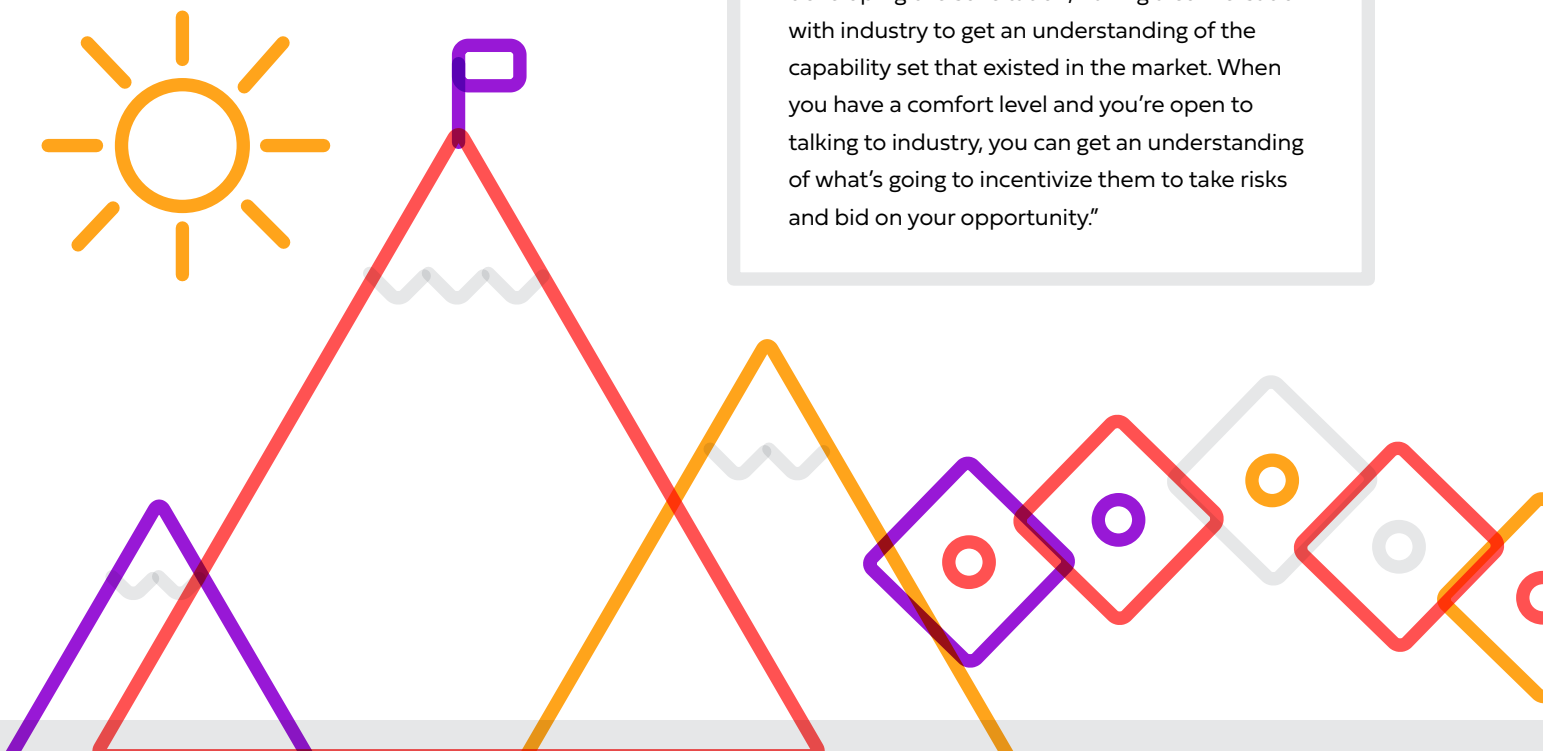
Although Arrieta's name has become synonymous with blockchain in government, he sees it and other emerging technologies as a means to an end. His philosophy is that organizations shouldn't outsource their brains to technology. Instead, they should use it to ask smarter questions.

His advice: Get an understanding of what your strengths are, what you understand really well, and try adding value in those areas using emerging technology.

“

I truly believe this: Without my understanding of acquisition, I don't think that I would have been able to proof, pilot and even scale on some level some of the capabilities that we've been able to put together.

When I was the industry liaison for DHS, we taught about myth busters and communicating with industry. I had done large solicitations, and I was much more comfortable with, before even developing the solicitation, having a conversation with industry to get an understanding of the capability set that existed in the market. When you have a comfort level and you're open to talking to industry, you can get an understanding of what's going to incentivize them to take risks and bid on your opportunity.”



Following that advice, Arrieta has used acquisition as a vehicle to explore how technologies such as blockchain and AI could help employees decide what work should remain in-house vs. being outsourced, and how much they should pay for that work based on historical data. The capability is called HHS Accelerate.

“

“Accelerate isn’t just about the blockchain. It’s a cloud capability that ingests and curates and shares data. We’re running a series of microservices. We used this approach called human-centered design to actually build it, and we touched 3,000 members in the acquisition workforce.

But we experimented and are currently using a recurrent neural network to provide visibility of the prices paid and terms and conditions [of HHS contracts].”

This recurrent neural network is a microservice of HHS Accelerate. It reads through terms and conditions and analyzes prices paid for contracts. It then clusters that information for acquisition professionals to use as part of their contract negotiations to get the best deal for the government.

“

“Is the data perfect and is the insight perfect? No. But it creates a discussion that’s very valuable and we think very interesting. We actually have used that to negotiate our first deal, and we believe if everybody uses it it’s going to save us \$30 million over five years. It’ll pay for more than double the effort that we put into HHS Accelerate thus far.”

As HHS looks to scale this capability, change management will be critical. From the onset, Arrieta and his team took a human-centered design approach to developing HHS Accelerate.

“

“We want to create an experience for people when they provide feedback in the human-centered design sessions. As you create an experience for folks, you will create a memory on a different way of doing business, vs. if you just train them on how to do business. If I tell somebody what to do, they remember, let’s say, 20%. If I tell them what to do, and then I put them through training as to why it’s important, maybe they remember 30%. But if I then go and have them do it, if I go and have them execute, they remember how to do it, and that’s how you change culture. So I think that’s the piece of experience that’s so important. That’s why folks want to go and bungee jump. That’s why folks want to travel.”

Arrieta credits his team’s successes with an openness at HHS to take chances, as long as they are managed. Before starting at HHS, he wrote a farewell letter to his colleagues at the General Services Administration that sums up the importance of risk-taking, even if those efforts fall short.

“

“I started the email writing about all the things that we tried — and that didn’t work. The point to them was, ‘Thank you for experimenting and trying these different things’. We didn’t spend a ton of money, but we did spend time. We spent time and energy trying different things. I literally highlighted all the things that I tried and that they partnered with me on that didn’t work. And then I said, ‘But we did have some things that did work.’ And we highlighted them. I’m a firm believer that things work because of what you learn in your failures.”



SECURE PRIVILEGE. STOP ATTACKS.

ACROSS THE ENTERPRISE · IN THE CLOUD · ON ENDPOINTS

Unsecured privileged accounts add risk to your business anywhere they exist - 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise - on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networkiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- FIPS 140-2
- NIAP certified

Learn about our Federal capabilities at:

CyberArk.com

©2020 CyberArk Software Ltd. All rights reserved.



ENABLING INNOVATION THROUGH PRIVILEGED ACCESS MANAGEMENT

An interview with Kevin Jermyn, Federal Customer Success Director, CyberArk

Government agencies have often seen security as an obstacle to the adoption of emerging technologies and strategies. The problem has been that traditional security solutions lacked the flexibility needed to adapt to changing requirements. But that mindset is changing, as agencies adopt security solutions that enable them to deploy new security measures quickly and easily.

To learn more about this shift, we spoke with Kevin Jermyn, Federal Customer Success Director at CyberArk, which provides privileged access management solutions. He highlighted three steps that agencies can take to improve the flexibility and effectiveness of their security strategy.

1. Reduce the overhead involved in managing access.

Traditionally, the deployment of a new managed access security solution requires setting up an entire server architecture, which is expensive, both in terms of upfront costs and long-term maintenance. A Software-as-a-Service (SaaS) approach changes that equation.

This is especially important when an agency needs to scale up and scale back access management services on demand – for example, to give remote partners temporary access privileges. Without a SaaS-based access management solution, that would be an administrative headache, Jermyn said.

With SaaS, agencies “can focus on managing their business operations – and do it in a secure fashion,” he said.

2. Simplify the management of application credentials.

Many agencies are modernizing their application environments by using automated IT infrastructure, containerization and DevOps methodologies. The challenge is that these approaches involve a wide array of non-person entities, such as vulnerability scanners, RPA platforms and Continuous Integration/Continuous Development (CI/CD)

tools. These entities should be issued credentials, just like developers.

That’s not easy, given the accelerated speed of the development environment, Jermyn said. **“Sometimes your development teams move to modern development cycles without considering the impact of credential sprawl.”**

You can simplify application credentialing by integrating the application credentialing manager with CI/CD toolsets and container platforms. “We allow developers to ensure that any credentials needed by their applications are provided in a secure and audited fashion,” Jermyn said.

3. Enforce least privilege at the endpoint.

Agencies should provide end users with access only to those specific network resources they need to do their jobs. This concept of “least privilege” is a way of reducing the risk of both accidental and malicious cyber disruptions.

End users – especially developers – often push for elevated permissions or even administrative rights. Otherwise, they say, they’ll need to go to the help desk for even minor requests, which can undermine productivity. But, in the wrong hands, elevated permissions mean trouble. “This can easily be exploited by an attacker as part of their attack cycle,” Jermyn said.

The key to enforcing least privilege is to combine several capabilities:

- Advanced privilege management, making it easier to manage, elevate and remove local admin rights without impacting productivity.
- Credential theft protection, protecting operating system browser and file cache credential stores.
- Application control, automatically blocking malware from running and reducing configuration drift on endpoints.

STATES EMBRACE NEW WAYS OF THINKING

Each year, NASCIO surveys state CIOs about their top priorities for the coming year. Although some topics are perennial (e.g., cybersecurity and cloud), the list serves as a good barometer of shifting concerns at the state level, with topics appearing and disappearing and appearing again. The 2020 list marked the debut of a new topic: “Innovation and Transformation through Technology.” To explore this further, we spoke with Meredith Ward, Director of Policy and Research at NASCIO.

GOVLOOP: Why are we seeing a growing interest in innovation or emerging technology in many states?

MEREDITH WARD: We still see some cultural resistance to change in state government, especially at the agency level. People have been doing their jobs in a certain way for a long time, and it’s just human nature to not want to do things differently. But we have this convergence of factors that states are facing right now.

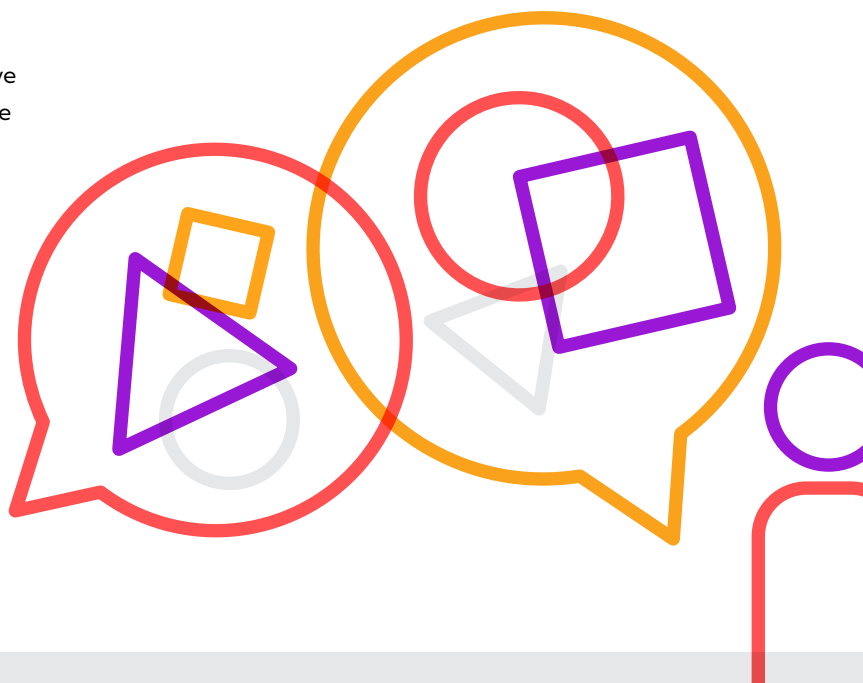
You’ve got the silver tsunami – an aging population – which means that you have a greater demand for citizen services, and which is also decreasing the size of available workforce. You’ve got states continuing to have constrained budgets and resources – still dealing with the aftermath of the recession. You also have states facing increased cybercrime, such as ransomware attacks at municipalities and state governments. On top of all of that, citizens expect to log in to one state website and have access to everything with a personalized, Amazon-like experience.

With all of that, states have to be looking toward innovative technologies. And not just technologies but also innovative processes – and innovative people who can solve these challenges and make all this work.

How important is it to get leadership buy-in for innovative projects?

At the state level, having the buy-in from a governor who’s committed to innovation is extremely important. And we’re seeing that that is increasingly common these days. In a report we did in conjunction with Accenture, we found that a large majority of governors are making innovation a priority. (See sidebar, p. 19.) That goes a long way.

At the agency level, that can be hard because of cultural resistance, but we do see that the role of the CIO has changed from one in which they do a lot of technical IT work – fixing problems and providing services – to a role in which they are more of a broker of services, using outside vendors to solve problems. We think that provides for greater innovation as well. The CIO can really go out and find the right solution on the outside for the agency, instead of just saying, “Well, this is what we have in office that we can provide for you.”



We've also seen a greater focus from CIOs on customer relationship management – how the CIO's office relates to the agencies it serves. Those relationships don't always come naturally, so a lot of CIOs are now hiring a Chief Customer Officer, or they have put in place plans to improve those relationships and take feedback, and to make sure they're doing more things face to face. And when you improve those relationships, then you can improve innovation as well.

Why do some agencies run into resistance when it comes to innovation?

We talk a lot about cultural resistance to change – it seems to be a recurring thread throughout everything I research here. You have people who are doing jobs that are kind of repetitive, and all of a sudden a technology comes along that can do that part of the job for them. You say, "Hey,

why don't you do this?" But it's different. It might end up being better, but they might not feel that way at first. This is something I think that a lot more of the workforce will be facing in the next few years as automation becomes more prevalent.

There's also risk aversion. Historically, people might have been afraid to try something new, or to speak up, to come up with new ideas. It's really important that the CIO take the lead in creating a safe place for innovation and in encouraging it and rewarding it – and in hiring people who are innovative thinkers. A lot of that goes a long way in changing the culture.

In state agencies, things tend to stay the same way for a long time, and so it might require a little discomfort for a while until people get used to things being different.

THE STATE OF INNOVATION IN STATES

In January 2020, NASCIO and Accenture released a report on the perspective of state CIOs regarding innovation. The survey of state CIOs focused on identifying current practices and their views regarding obstacles to innovation.

63%

of respondents cited lack of funding as the top barrier to innovation.

49%

said they have governance structures to oversee innovation.



31%

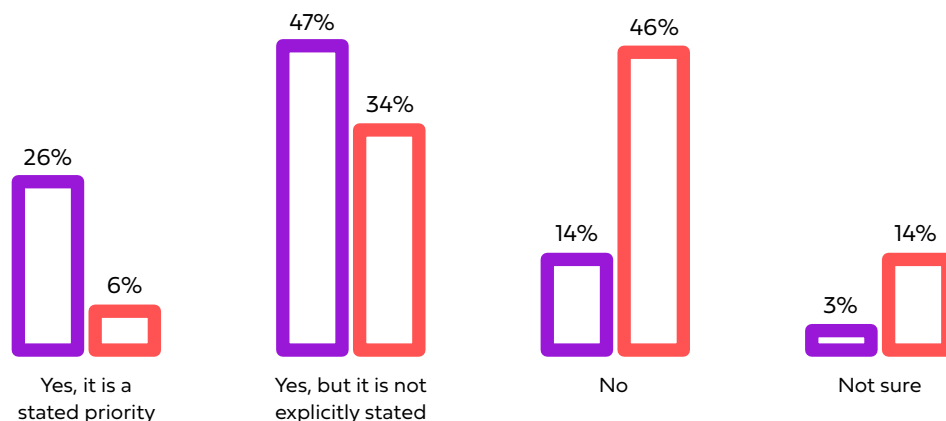
said they were developing governance structures.

85%

cited struggles finding the right skills for innovation.

Has the current administration/legislature of your state made innovation a priority?

 Administration
 Legislature





Today's Transformation for Tomorrow's Innovation

Dell EMC Data Protection solutions helps agencies transform their data centers to enable greater operational efficiency, resiliency and scalability throughout the entire infrastructure – from edge to core to cloud.

Cloud Solutions »

Meet your most stringent recovery objectives while protecting traditional and emerging workloads across your multi-cloud environment.

VMware Solutions »

Dell EMC Data Protection is architected for the modern, software-defined data center with industry-leading VMware integration.

Cyber Recovery »

Protect your organization's most critical data from destructive cyberattacks with a secure vault and enable rapid recovery with intelligent analytics and automated management.

DELLTechnologies

www.dellemc.com/dataprotection

CLOUD PROVIDES COST-EFFECTIVE SOLUTION TO DATA BACKUP, RECOVERY CHALLENGES

An Interview with Brad Montgomery, Senior Manager, Federal Presales, Dell EMC

Agencies can't afford not to have a strong data backup and recovery strategy. That's just a given. The challenge is coming up with a strong backup and recovery strategy that they can afford to maintain as their data requirements grow and evolve. That is why the cloud has emerged as the platform of choice for data backup and recovery. To learn more, GovLoop spoke with Brad Montgomery, Senior Manager for Federal Presales at Dell EMC. He discussed three different use cases for cloud-based data backup and recovery.

Backing up on-premises data in the cloud

The case for backing up data from on-premise systems to the cloud is straightforward, Montgomery said: it's cost-effective and simple. As the volume of data grows, agencies are spending more and more money on both their primary storage systems and their backup systems. Over time, they will spend additional money managing, maintaining and upgrading those backup systems. It's a daunting scenario.

By backing up data to the cloud, agencies can get out of the business of buying and maintaining hardware, leaving those worries to cloud services providers. In the process, they can shift funding from capital expenditures (CapEx), which cover the purchase of assets, to operating expenditures (OpEx), which cover the purchase of on-going services. CapEx budgets typically are less predictable year to year than OpEx.

Backing up cloud-based data in the cloud

Market research firm IDC has predicted that 49% of data will be stored in public cloud environments by 2025. Although that means agencies won't need to worry about managing and maintaining a lot of infrastructure, they still need to think about data backup and recovery. Even

if a cloud service includes backup and recovery, those capabilities might not be sufficient.

"In particular, when evaluating cloud data protection services, pay attention to how backup is architected in the Cloud," Montgomery said. "For example, many backup providers rely heavily on block storage, which is higher performing and more expensive than necessary for backup purposes."

Also, public cloud services likely do not include robust deduplication capabilities, which keeps down storage costs by eliminating redundant copies of data.

Disaster recovery to the cloud

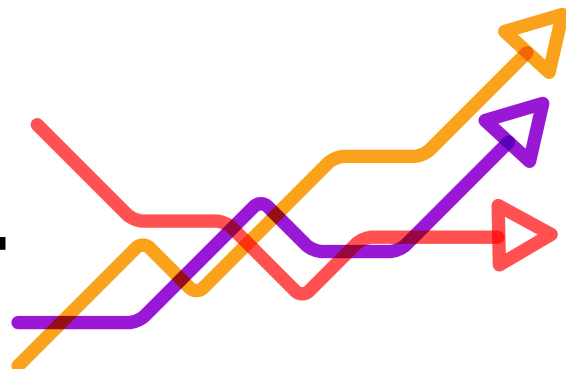
When it comes to disaster recovery, the cloud can bring some much-needed simplicity to what is an inherently-complex operation.

Cloud-based disaster recovery (DR) allows an agency to copy backed-up virtual machines from their on-premise environment to the public cloud for the orchestration and automation of core DR operations: testing, fail-over (moving from the primary site to the backup) and fail-back (moving back to the primary site). Most importantly, the cloud accelerates the time to recovery.

Finally, by using the same cloud-based capabilities for all three of the scenarios described above, an agency provides a more consistent user experience.

"You want to be able to simplify your operations and improve the cloud economics through a consistent management experience across all the clouds you have," Montgomery said.

8 AREAS OF PROGRESS & IMPROVEMENT IN GOVERNMENT TECH



In his keynote at GovLoop's "Gov's 2020 Tech Focus" virtual summit, Craig Fischer, a Program Manager at FIT within the Bureau of the Fiscal Service, discussed four areas where the government is currently doing well, along with four areas in which it could improve going into the 2020 technology landscape.

WHERE THE GOVERNMENT DOES WELL

1. Starting small and starting simple

With the excitement that surrounds new technologies, it's easy to get ahead of ourselves. Fischer cautioned against letting our eyes become bigger than our stomachs and going after technologies without a plan.

Instead, he recommends breaking projects down into smaller chunks and then choosing the right piece of technology. Instead of tasking IT teams with tackling a new technology full stop, provide them with smaller, actionable areas where they can implement the right solution bit by bit.

2. Finding comfort in the unknown

Fischer shared that in his experience, every technology project has taken some kind of unexpected turn. Although that's common across many fields, it is especially so for teams working with new and emerging technologies. Fischer urged teams to accept this reality and expect the unexpected in their project plans. Exploring the possibilities of the unknown is a huge part of the process and approaching each case as an opportunity to learn can yield only more fruitful results.

3. Practicing radical transparency

Fischer acknowledged that sometimes teams, including his own, have kept their work on new projects under a cloak of secrecy before involving others and getting leaders on board, but this can be extremely counterproductive. Teams should allow themselves to be more outcome-independent when exploring the uses of new technologies, Fischer said. The whole process will benefit from having more eyes and more perspectives involved.

4. Appointing designated teams

Because of the ever-growing vastness of the emerging tech field, Fischer stressed the importance of having separate teams dedicated to proactively searching for and implementing new technologies. These teams should scan the news and reports from other agencies about new technologies. In addition, they should constantly analyze the agency's processes and never stop asking, "How could these be improved?"

WHERE THE GOVERNMENT COULD IMPROVE

1. Absorbing the pace of change

From AI to blockchain and RPA – not to mention the remaining galaxy of technology making its way into the mainstream – describing the amount of change government IT departments face as “overwhelming” would be a massive understatement. Fischer said that moving forward, it’s imperative that agencies take a tactical, critical approach to modernization and selectively prioritize certain projects to protect their spread-thin IT departments from overload.

2. Keeping up while technology leads the pack

At this moment, technological progress is vastly outpacing current policies, practices and, sometimes, even laws, Fischer said. If we want to see these new technologies successfully find a place in government, agencies must find ways to be adaptive and better negotiate how to fit new tech into the rigid structures that have already been established, he added.

3. Confronting organizational cultures

Many agents of change support modernization efforts, but Fischer noted that there are also many employees who oppose change. It can be very challenging to get these individuals on board with new projects, especially if they lead the decision-making process.

One strategy that Fischer emphasized is that when you are describing a new technology pilot to leaders, do not focus on how it works. Instead, highlight the technology’s specific, tangible benefits and how it will improve mission-critical processes.

4. Fostering cross-agency collaboration

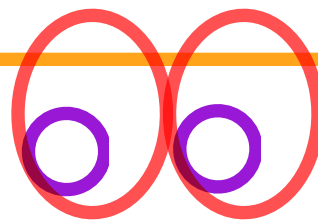
Agencies don’t regularly share projects, use cases or lessons learned, Fischer said. Because of the challenging pace of emerging technology, he said that there is immense value to be gained by exchanging this information and that the implementation could be revolutionized at all levels of government.

BEST PRACTICE: CULTIVATING A ‘SCANNING’ CULTURE

At GovLoop’s “Gov’s 2020 Tech Focus” virtual summit, Fischer discussed the importance of making it a practice to always monitor the media and other sources for new and emerging technologies and tech strategies.

Fischer said that he first started paying attention to blockchain after reading an article in the Wall Street Journal about how the technology was working in the finance space. That got him thinking about how it might work in the federal domain, which led to more focused research, a presentation to agency executives and eventually blockchain pilots.

“One of the things that I think you have to do is make this scanning part of your organizational culture,” Fischer said. “It just has to be part of the job that you do – always being on the lookout.”





Don't let legacy technology get in the way of the future

Astadia is the industry leader for mainframe transformations. We modernize millions of lines of mainframe code every year for Government Agencies.

- 25 years experience
- Mainframe to cloud focus
- 200+ successful projects

Migrate your mainframe to the cloud

[Watch our video series with Micro Focus Gov >](#)

[Learn how Astadia works with Government Agencies >](#)

[Contact us >](#)

MAINFRAME MODERNIZATION: PAVING THE WAY FOR NEW POSSIBILITIES

An interview with Steve Steuart, Chief Technology Officer, Astadia, and Kevin Hansen, Chief Technologist, Micro Focus Government Solutions

Sooner or later, agencies need to confront a hard truth about their legacy mainframe environments: While the mainframe is a reliable, stable platform, it is not exactly a hotbed of innovation. If agencies want to take advantage of the latest technologies, such as artificial intelligence, containerization and advanced analytics, they should look to the cloud.

With that in mind, we spoke with Steve Steuart, Chief Technology Officer at Astadia, and Kevin Hansen, Chief Technologist at Micro Focus Government Solutions, whose companies have teamed to help agencies move mainframe assets to cloud-based platforms. They recommended approaching such a move in three phases.

1. Conduct application estate analysis

The first step is to assess your existing applications, associated processes and infrastructure to highlight the value and impact of migrating your mainframe environment to the cloud. Automated tools can help assess application inventories, infrastructure dependencies, cloud readiness/maturity and other related components and processes.

One of the goals is to understand what needs to be migrated – and what can be left behind. That can be a daunting task. Most mainframe environments have been around for decades, and they likely include many applications and processes that have outlived their value, Steuart said. You need to make rational choices about what you really need – about what aligns with the needs of the operation.

2. Prioritize generating savings quickly and reducing risk

The most proven approach to moving workloads off the mainframe is to do a “lift and shift” –rehosting (recompiling) an application as-is to the cloud. Lift-and-shift is sometimes frowned on, because such applications don’t take full

advantage of cloud capabilities. But when used as an incremental modernization step, it offers an extremely pragmatic approach, especially from a financial perspective.

Because most legacy mainframe platforms are based on proprietary technology, they are inherently more expensive than cloud and other platforms that are based on commodity technology. Once these applications are rehosted however, many options open up to expose COBOL code to modern languages and API or micro service architectures.

Re-hosting “provides a really low-risk approach and quick time-to-value, for existing mainframe workloads,” Hansen said.

3. Continuous application modernization

But agencies will achieve even greater benefits by continuing to modernize the applications once they are rehosted in the cloud, making it easier to leverage new technology and innovations.

Continuous modernization options include refactoring or restructuring the code to improve its performance, exposing application transactions as web services, or even rewriting the application altogether. Agencies also might move to a continuous integration/continuous delivery model, in which new capabilities are delivered incrementally on a regular basis, rather than as part of a big-bang-style product update quarterly or annually.

The overarching goal is to keep applications evolving as requirements evolve, rather than trying to play catch-up every five or 10 years.

“Work on continuous modernization,” Hansen said. “It’s not a project you do once, and you’re done. It’s an on-going journey.”

BEST PRACTICES

THE NAVY'S PLAYBOOK FOR PLAYBOOKS

NavalX describes itself as the as workforce “super-connector,” focusing on bringing new technologies and methods to the DON workforce. One of its primary tools is playbooks, which are designed to help Navy organizations adopt a given technology. GovLoop spoke with Kevin Burnett, a Pioneer in Residence at NavalX, about the art of creating playbooks.

One key issue: The playbook needs to be as easily relatable as possible for readers.

“

For example, if it's a use case, how can they repeat the success of your use case? If you're providing them guidance, how do you characterize that guidance to the lowest common denominator of your consumer so that it's relevant for everyone? It's all about showing results. For example, you discuss a process that once took 300 days, and how after you applied the process described in the playbook, it took less than half that time. That's a very important attribute for people to be able to latch onto, because they say, 'Oh, I have a good sense of being able to get 2x or 4x or 10x.'”

But there's a fine line between being too generic and too exact, he said. For example, if you discuss the technology using a very specific use case, and that use case is not relevant to the reader, they'll stop reading. But if the use case is too generic, it won't have enough context for the reader to gain meaningful insight. Somewhere there's a sweet spot.

“

I like to say it's a 'free space' vs. 'gravity' scenario in which industry teaches a discipline in free space and we give additional context for how to apply Department of Navy gravity to it to better enable the consumer to apply it in their particular organization. Take something like cloud. There are a lot of implications when using the cloud in the Department of Navy in terms of cybersecurity, management, resources. That's the gravity we try to convey in our playbook.

But it can quickly get into the weeds, to the point where you might lose your consumer. That's why, for the more complicated components of a playbook, we're starting to look at things beyond just wikis for conveying that information. We're starting to work with podcasts as well as animated sketches, video-based vignettes – basically coming up with a multimedia or alternative distribution channel for that more complex content.”

EMERGING TECHNOLOGY ADOPTION:

QUESTIONS TO CONSIDER

In December 2019, GAO published a report that outlines key factors to consider when assessing the potential impact of new technology.

The “Technology Assessment Design Handbook” is geared primarily to GAO’s own staff, which conducts assessments on behalf of Congress. However, they believe those practices might have value for other agencies and organizations looking to bring more rigor to their technology assessments.

Here are key questions that such assessments might consider.

DESCRIBING STATUS AND CHALLENGES TO DEVELOPMENT OF A TECHNOLOGY

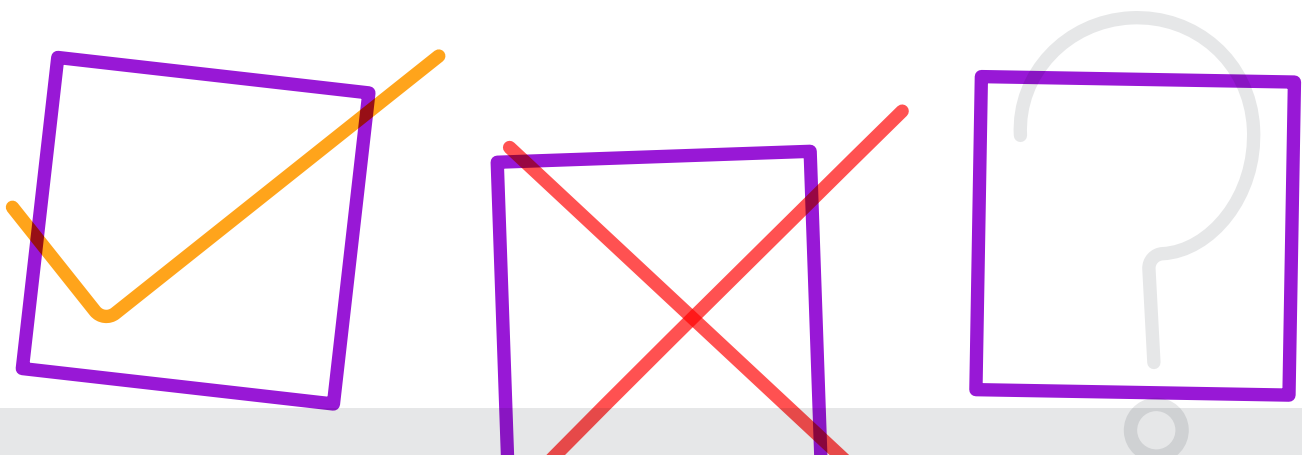
- What is the current state of the technology?
- What are alternative applications of the technology?
- Does the status of technology vary across different applications or sectors where technology is being developed?
- What are technical challenges to the development of the technology?
- What technologies are available or under development that could address a specific problem or issue?
- What challenges do these technologies face?

ASSESSING OPPORTUNITIES AND CHALLENGES THAT MAY RESULT FROM USE OF A TECHNOLOGY

- What are the expected or realized benefits of the technology?
- What unintended consequences may arise from using the technology?
- Do uses or outcomes of the technology differ across geographic, economic, or other social groups or sectors?

ASSESSING COST-EFFECTIVENESS AND POLICY CONSIDERATIONS RELATED TO USE OF A TECHNOLOGY

- What are the economic and effectiveness impacts of implementing specified technologies?
- What are policy implications resulting from advances in the technology?
- What policy options could address challenges to the use of a technology to achieve a specified outcome?



CONCLUSION

WHAT'S NEXT?

Without a doubt, something is shifting in the public sector. Not that long ago, the prevailing wisdom was that government agencies could not afford to risk using emerging technologies or strategies until they were well-proven in the private sector. That is no longer the case, and for good reason.

First, agencies are beginning to realize that, in some cases, they cannot afford not to take advantage of emerging technologies. For instance, when they:

- Are dealing with intractable problems that existing solutions do not adequately address.
- Would otherwise miss out on making significant gains in efficiency and effectiveness with existing services.
- Have an opportunity to create new services to achieve their missions.

The need for risk-avoidance also has been tempered by the realization that risk can be mitigated. That shift in mindset is significant and reflects the growing importance of technology in agency operations.

Because technology is increasingly seen as critical to agency operations and missions, agency leaders are bringing more discipline to its adoption, use and management. Practices in areas such as risk and change management can help agencies identify and address challenges early in the process.

A growing number of agencies also are getting wiser about doing proofs-of-concept – small-scale projects designed to test how a technology works, the benefits it can achieve and the pitfalls to avoid. The better that agencies get at designing proofs-of-concept, the fewer risks they will face in the future.

Still, none of that is to say that agencies can eliminate the risks associated with emerging technology; that's not realistic. The goal should not be to avoid risk but to manage it effectively.

That's the real take-away here. In the coming year, your agency is likely to take a close look at one or more of the six technologies highlighted in this guide. But the overarching goal should be to develop a strategy for making the adoption of emerging technology both a well-honed discipline and an essential element of the broader IT strategy.



ABOUT

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | [@govloop](https://twitter.com/govloop)

THANK YOU

Thank you to Astadia, Automation Anywhere, Carahsoft, CyberArk, Dell, immixGroup, Micro Focus and Red Hat for their support of this valuable resource for public sector professionals.

AUTHORS

John Monroe, Director of Editorial
Nicole Blake Johnson, Managing Editor
Isaac Constans, Staff Writer
Mark Hensch, Staff Writer
Pearl Kim, Editorial Fellow

DESIGNER

Kaitlyn Baker, Creative Manager



1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop

