



SIMPLE • SEAMLESS • SECURE

# The Path Toward Intelligent Transformation



servicenow

Step by step, federal agencies are progressing from digitization and automation to transformation. The goal is not to modernize one particular application or automate one particular process, but to transform the delivery of services from end-to-end.

Transformation means addressing all aspects of service delivery, from digitizing and automating manual processes and improving the user experience to boosting cyber defense capabilities.

Increasingly, transformation is built on an intelligent platform, which brings together a wide range of capabilities enhanced with artificial intelligence (AI) and governed by a common architecture and a common data model. **The platform approach ensures that enterprise services and operations are simple, seamless and secure.** This is the goal of intelligent transformation.

An important byproduct of these activities is increased trust. When the public interacts with a government agency and has a great experience, their trust in government increases. When the government invests in cybersecurity, the public's trust increases. When the government explains how new AI tools make decisions that affect the public, trust increases. With trust in government at an all-time low, these activities have never been more important.

During ServiceNow's recent Federal Forum, government and industry leaders gathered to discuss strategies for delivering on the promise of intelligence transformation and building trust. This report looks at six key actions for government leaders that emerged during that discussion:

1. Lay a Solid Foundation for Digital Transformation
2. Foster a Culture of Innovation
3. Think in Terms of the Total Experience
4. Put Strong Governance in Place for AI
5. Understand the Potential and Pitfalls of GenAI
6. Build Better Cyber Resilience Through Automation

# Lay a Solid Foundation for Digital Transformation



SIMPLE • SEAMLESS

**Venice Goodwine**, Chief Information Officer, U.S. Air Force

**Chris Bedi**, Chief Digital Information Officer, ServiceNow

One of the most important projects Goodwine has undertaken during her tenure as CIO of the Air Force was taking a complex array of disparate systems and integrating them through an intelligent platform, simplifying and streamlining its operations.

The platform enables the CIO organization to deliver relevant information to warfighters at what Goodwine calls the speed of relevance and mission — something that requires integrated information, intelligence and processes.

“If we can eliminate governance blind spots, and have more consistent, reliable processes that produce measurable results, we have hit a homerun,” she said.

The adoption of the ServiceNow Platform provides an important foundation block for digital transformation. It incorporates modern tools like AI and machine learning to automate tasks, optimize processes and address requirements around security, privacy and compliance. And it can do it at scale.

“A platform that can scale to meet the workload of thousands and millions of transactions per hour, and is secure, with encryption and all the techniques that you need to make sure your data is protected—all of this can accelerate the outcomes you can drive,” said ServiceNow’s Bedi.

While embracing a single intelligent platform is the best way to ensure fast, accurate decision-making and productivity, old habits can die hard. To overcome the hurdle, Goodwine focused on demonstrating the value and outcomes that the platform would provide. Whenever possible, that includes hard numbers.

“I can’t yet show them that if they use this platform they will save 50 FTEs, but I can show them that when they go into a meeting, you don’t have to create PowerPoint slides. You can just read it from our dashboard. You can manage your entire product in the portfolio module of the platform.”

Over time, intelligent platforms will only get more intelligent and more useful, Bedi said.

“We’re getting to the point where the platform will be proactive,” he explained. “For example, the chatbot will tell you that the average life of a laptop is 32 months and you’re at month 28. It will tell the user that they have been rebooting a lot in the last two weeks and ask whether now would be a good time to replace the laptop.”

Now that the platform is fully implemented, Goodwine is working hard to expose users to it.

“Start using the tools and let others watch. Show them the benefits you’re getting, and they will start asking questions,” she said. “The more they ask questions, the more you can start bringing them in. That’s how you build the coalition of the willing.”

***“If we can eliminate governance blind spots and have more consistent, reliable processes that produce measurable results, we have hit a homerun.”***

**Venice Goodwine**, CIO, U.S. Air Force

# Foster a Culture of Innovation



**SIMPLE • SEAMLESS • SECURE**

**Reshea Deloatch**, Executive Director of the Solutions Development Directorate within the Office of the CIO, Department of Homeland Security (DHS)

**Lorelie Diestro**, Deputy Director of Digital Innovations at the Center for Naval Analyses

**CDR Jonathan White**, Cloud, Data and AI Branch Chief, Coast Guard's C5ISC Infrastructure Services Division

**Jesse White**, CEO, Intact Technology



Intelligent transformation is not the same as modernization. Modernization is about updating old technology, making it possible to work more quickly and effectively. Transformation is about tackling old problems in new ways or delivering new services altogether — always with a focus on making those services simple, seamless and secure. In other words, it's about innovation.

The challenge, then, is to foster a culture of innovation — one in which both leaders and employees embrace and even drive change. Here are three key ways to do that.

## 1. Build on a Foundation of Digitization

In the past year, CNA, an independent research and analysis organization focused on the nation's safety and security, has digitized 26 formerly manual workflows and forms in its service catalog.

This has enabled CNA to provide employees with faster, more effective services, including self-service options, CNA's Diestro said, which has contributed to significant improvements in workforce productivity and efficiency.

"Manual processes were holding us back from progress," Diestro said. "Now we can reallocate our employees' time to tasks and activities that are far more relevant and productive."

With digitization under control, agencies can focus on change management, ensuring that everybody understands what's coming and how it will make their lives better, said Intact's White.

"Everybody needs to understand what's coming and how it will make their life better," he said, "because it's actually not fear of change; it's them being afraid of what change may mean for their job."

## 2. Build on a Foundation of Data

Data is the key to innovation. With it, agencies can improve decision-making, create new products and services, personalize experiences and improve operational efficiency. But there's a catch. To be of any use, data must be clean, current, transparent and shareable.

To accomplish this goal, the Coast Guard is embracing the concept of a data mesh, which is a decentralized approach to data architecture and governance.

"We're establishing data domain owners and empowering them to own, classify and deal with their own data, and then serve it back to the organization as data products," CDR White explained.

At CNA, data is everywhere. Behind the service desk, for example, is a wall of TV monitors that display dashboards, reports and data in real time, including the status of key performance metrics.

"With the right data, our leadership can make well-informed and actionable decisions and identify growth opportunities," Diestro said.

## 3. Take Calculated Risks

Deploying a large system that changes how people work is always a risky venture. But there's something to be said for taking calculated risks.

The Transportation Security Administration, which is under the auspices of Homeland Security, approaches such situations as a learning moment — deploying solutions and then observing how TSA and the public reacts to those solutions.

"We're making sure that folks aren't afraid to deploy solutions and then take a step back to see if they are working, and enhance them in the process," DHS' Deloatch said.

# Think in Terms of the Total Experience



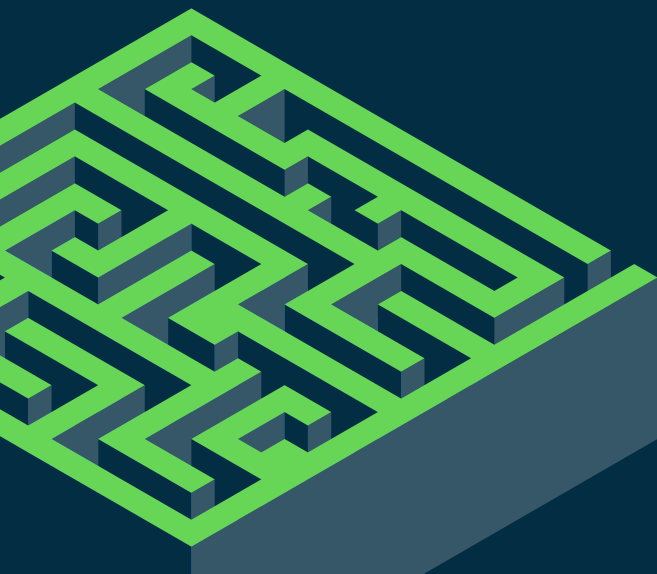
## SEAMLESS

**Javier Inclán**, Assistant General Manager and CIO, Office of Inspector General, National Science Foundation (NSF)

**Mark James**, Director of the OIT Enterprise Cloud Services Division, U.S. Customs and Border Protection (CBP)

**James Johnson**, Program Executive Officer, Information Operations, Defense Logistics Agency (DLA)

**Col. Kris Saling**, Acting Director, Innovation Directorate, U.S. Army Recruiting Command



When the concept of the customer experience first emerged, most organizations saw a clear distinction between the customer or constituent experience and the employee experience. But that mindset is rapidly changing.

According to a [recent survey](#) by ServiceNow and Thought Lab, 35% of public and private sector organizations globally improved service quality by aligning the customer and employee experience. That number is expected to grow to 43% by this year.

That survey pinpoints how important it is to consider and combine the experiences of all users — employees, customers and partners. Incorporating the needs and priorities of all of these user groups is the key to building effective cross-functional processes and delivering more effective and seamless experiences.

## Understand Your Different Types of Users

CBP's James recommends leaving no stone unturned when it comes to gathering information on your different types of users.

"For anyone going on this journey, don't just follow the legacy data. Look at data from your tools for employee or customer experience like event logs and mission reports," he said. "These are places where you might see either the frustration or the acceptance of the way processes and how things are flowing within the organization."

It's also important to examine each segment of the user experience separately, said Col. Saling, with the Army Recruiting Command.

**35%** of organizations globally improved service quality by aligning CX and EX

"If we look at each segment of the soldier experience by itself and not in context, we're going to have problems with authorities, problems with the underlying data architecture, and all the different pieces of what we need to implement these programs," she said.

The Army is currently working diligently to address this issue by working with partners to examine how it structures the total soldier experience.

Developing a clear strategy is key along this path, NSF's Inclán added. "It's really important to think about what's next. What are the things that we could do to help our customers, our colleagues, other employees, to do their jobs better?"

NSF recently did just that, bringing the IT team together with its data operations group for a full-day strategy session.

## Create a Seamless Experience

"We use the word 'intentionality' a lot: making sure we're communicating an intentional way," Inclán said. And while NSF is making good progress, there are occasional bumps along the way. "In customer experience especially, we have to have thick skins and not take things personally," he said.

To ensure user-friendliness and buy-in, DLA leaders include as many of its 25,000 employees in workshops as possible to help shape and frame their experience.

"For DLA, the biggest benefits have yet to be realized," Johnson added. We'll be able to reduce IT inventory and costs while delivering a common user experience across multiple platforms. There are some real challenges to getting there, but we will get there."

# Put Strong Governance in Place for AI



SECURE

**Brian Peretti**, Deputy Chief AI Officer and Director of Domestic and International Cybersecurity Policy, U.S. Department of Treasury

The White House's [Executive Order](#) on artificial intelligence addresses both the extraordinary promise and potential dangers of the technology. Used responsibly, AI can help solve big problems. But it can also foster fraud, discrimination, bias, disinformation and pose risks to national security.

The White House has asked the Secretary of Treasury to advise financial organizations on the appropriate use of and best practices for AI while managing risks. While the focus is on the financial sector, some of the lessons apply to agencies as well, as they work to deploy AI responsibly and securely.

The department started by interviewing 42 financial firms of various sizes to understand how AI is being deployed and the challenges these firms are experiencing. The department concluded that while there is no new risk because of AI, the technology does provide a different vector for criminals to exploit.

It's opportunity versus challenge, said Treasury's Peretti.

"People are still trying to steal information and use insider threats to cause problems, and AI can amplify that." At the same time, he said, models are being trained to help prevent those attacks. A new generation of firewalls, for example, use AI to train threat detection models and can fix issues in real time.

Still, the risks are real. The key is strong governance.

Based on the recent study, Treasury has appointed a Chief AI Officer, Peretti said, somebody who "owns this risk, who understands this risk, and who is able to really be an advocate, both on the positive and negative side of AI."

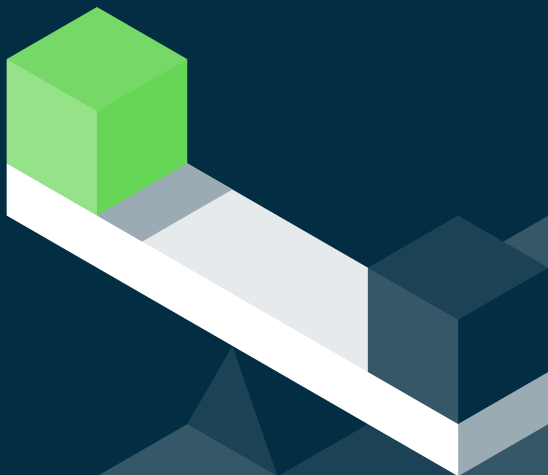
The department also is establishing a governance board. The board will work to understand different use cases for AI, such as reducing fraud. The goal, Peretti said, is to focus on use cases that use AI to spot trends before they exist and prevent bad acts from happening before they happen.

The study also recommends that the department combine forces with the private sector to develop ways of using AI. Over time, Peretti expects that the public-private partnership will yield good information for other sectors to adopt.

"AI isn't good or bad, it's just there. It's about using it in the right way to get to the right spot," he said.

***"AI isn't good or bad, it's just there.  
It's about using it in the right way to get to the right spot."***

**Brian Peretti**, Deputy Chief AI Officer and Director of Domestic and International Cybersecurity Policy, U.S. Department of Treasury



# Understand the Potential and Pitfalls of GenAI



SEAMLESS • SECURE

**Alexis Bonnell**, CIO, Director of the Digital Capabilities Directorate, Chief AI Officer, Air Force Research Laboratory (AFRL)

**David Larrimore**, Executive Director of the Chief Technology Officer Directorate for the Department of Homeland Security, Office of the Chief Information Officer (CIO)

**John Lau**, Senior Strategic IT Operations Adviser, U.S. Patent and Trademark Office (USPTO)

**Catherine Manfre**, Chief Technology Officer, Office of Personnel Management

Generative AI is on everybody's radar right now, and with good reason. Already agencies are deploying it to help employees automate routine tasks and improve their efficiency. Given time, it is expected to reshape how people work and revolutionize government services — the epitome of intelligent transformation.

The National Institute of Standards and Technology (NIST) recently published a new [resource](#) to help organizations evaluate and measure GenAI capabilities and limitations. More recently, NIST published a [draft publication](#) to help organizations manage the risk of Generative AI, both in security and privacy.

The key is to balance the promise and the pitfalls.

## Prepping the Workforce

The first step is demystifying GenAI. "It's not there to replace people or jobs," USPTO's Lau said. The agency is approaching the issue by creating an AI lab where employees can test and get used to the technology.

Focusing on people is a smart move, Manfre added. To help agencies do that, the Office of Management and Budget has developed the [Workforce of the Future](#) playbook, which both explains the potential of AI and how employees are likely to interact with it. It includes a specific section on how generative AI can improve efficiencies in areas like hiring processes and upskilling the workforce.

It's also the time to hire and train AI specialists. DHS, for example, is currently hiring AI experts to fill new positions like AI Technology Expert. Its AI Corps initiative aims to hire 50 AI experts across the Department. "Once we bring those experts in, the work starts solving high-priority mission issues," Larrimore said.

## Security, Responsibility, Risk

As part of that effort, agencies need to educate their employees on the concept of responsible AI, ensuring that AI is always used in ways that are both ethical and legal.

Aim for responsible AI from Day One, AFRL's Bonnell said. "Our technology choices are as much about a manifestation of our values and culture as they are any particular capability," she said. "The normal morals and ethics should be extended to any tool we use, including AI."

DHS Security is taking the responsibility aspect seriously, using a multiple rung approach to cyber hygiene. Larrimore's team first drafted policies, working with its Office for Civil Rights and Civil Liberties as well as its Office of Science and Technology. The Department also created an AI task force, which in turn instituted the Responsible Use Group.

"The Department of Homeland Security has been using AI for over a decade, but the real difference is that we're now being intentional about it," he said.

**"Our technology choices are as much about a manifestation of our values and culture as they are any particular capability. The normal morals and ethics should be extended to any tool we use, including AI."**

**Alexis Bonnell**, CIO and Director of the Digital Capabilities Directorate, AFRL



# Build Better Cyber Resilience Through Automation



SECURE

**Bob Cunningham**, Executive Director, Enterprise Command Operations, U.S. Department of Veterans Affairs (VA)

**Richard Driggers**, Cyber Practice Lead, Accenture Federal Services

**Savanrith Kong**, Customer Experience Officer (CXO), U.S. Department of Defense

**Dr. Tiina Rodrigue**, Chief Information Security Officer, Consumer Financial Protection Bureau (CFPB)

**Davon Tyler**, Chief Information Security Officer, U.S. Department of Education Technology Directorate Office of Federal Student Aid (FSA)

Federal oversight organizations know all too well the challenges agencies have in keeping data and systems secure. During the past few years, plenty of directives have come out requiring agencies to take significant measures.

The most effective way to improve security and meet mandates is by automating security — everything from risk assessment, alert processing and incident management to insider threat management and threat hunting.

Automation is a force-multiplier. It enables teams to quickly spot threats, expose and prioritize the most critical vulnerabilities, streamline communications about threats and resolutions, and collect data on trends, risks and security operations.

## Don't Rush to Automate

But before jumping into automation, agencies need to do some prep work, experts said.

One of the most important steps, both before undertaking security automation and afterwards, is assessing the zero trust maturity level of the organization, Accenture's Driggers said.

"Agencies need a comprehensive security assessment of their cybersecurity posture across the enterprise," he said. "Once you have that, you are much better able to build a strategic roadmap of solutions of actions to take and really track your progress.

By making these changes upfront, agencies can start with a cleaner slate that eliminates fragmented areas of information, said CFPB's Rodrigue. "This leaves truly executable information that can be orchestrated and automated."

When you're ready to automate, don't get locked into any one vendor's solutions.

"When we automate, we're focused on removing barriers for asking various questions that come from cyber operations teams," FSA's Tyler explained. "We've done that by deploying vendor-agnostic tools that can integrate with other tools and toolsets. This allows us get questions answered faster and better about what's going on in our environment and quickly remediate what we see."

## Focus Less on Function, More on Outcome

During that upfront work, it is essential to think about security from the user's perspective. What does a good outcome look like to them?

"For us to really deliver to the warfighter, we have to understand the environment they are in, the conditions they are working under, the technologies they are using and the challenges they have," Kong said.

For DoD, that means reorienting the conversation from the functions of zero trust, or whatever solution is being considered, to mission outcomes. "And then we can apply things like zero trust in a more meaningful way that can have a much greater impact at scale."

VA is another agency determined to focus on customers and their outcomes.

"Everything we look at from a technology point of view is how will it make the job of the person helping the veteran better," VA's Cunningham said. For example, the agency has provided its service desk with robotic process automation, which can handle many basic tasks, such as password changes.

Security needs to be part of the discussion any time you're talking about automation. "If you're not thinking about security from the beginning, you'll find out about it when you begin having issues on the back end," Cunningham warned.



## Conclusion

---

The concept of intelligent transformation reflects an evolution in how agencies think about technology. In years past, they focused on updating products and capabilities — digitizing, modernizing, automating and securing.

Intelligent transformation shifts the focus from the means to the end. How do you take advantage of these new capabilities and deliver better outcomes, both for the agency and for the constituents they serve? Doing so builds trust inside and outside the agency.

In this way, the concept of intelligent transformation can help agencies think about artificial intelligence. Looking at technology investments, especially AI, through a lens focused on outcome, agencies are in a much better position to assess both the promise and the pitfalls, the use cases and the risks. This combined with a focus on Total Experience and cybersecurity positions to drive meaningful change.

**This is how transformation happens. Simple. Seamless. Secure.**



servicenow®