ICIT

The Institute for Critical Infrastructure Technology (ICIT)

Mission-Ready Modernization: Harnessing AI and Data for Secure, Efficient Government Transformation

Thank you to our Partners

CyberRisk ALLIANCE

Rocket® software

Executive Summary

Hosted by the Institute for Critical Infrastructure Technology (ICIT) and co-sponsored by Rocket Software and MFGS, Inc., "The Future of Government Data, AI Automation & Mission-Ready Modernization" brought together distinguished figures from the defense-focused public and private sectors.

Federal agencies face intensifying pressure to modernize systems, meet evolving citizen expectations, and manage costs—all while navigating a critical shortage of mainframe expertise and the complexity of moving mission-critical data across diverse platforms.

Against this backdrop, this whitepaper provides federal decision-makers with a roadmap to adopt automation and AI responsibly, securely, and in ways that align modernization efforts with mission resilience. Rocket Software and MFGS, Inc bring proven solutions in enterprise modernization, data agility, and AI readiness, helping agencies translate these priorities into mission-ready action.

Session participants

Michael "Mick" McCabe, Chief Data and AI Officer, Office of the Undersecretary of Intelligence & Security, Department of Defense

Doug Johnson, Vice President of Product Management, Rocket Software

Kevin Hansen, Chief Technology Officer, MFGS, Inc.

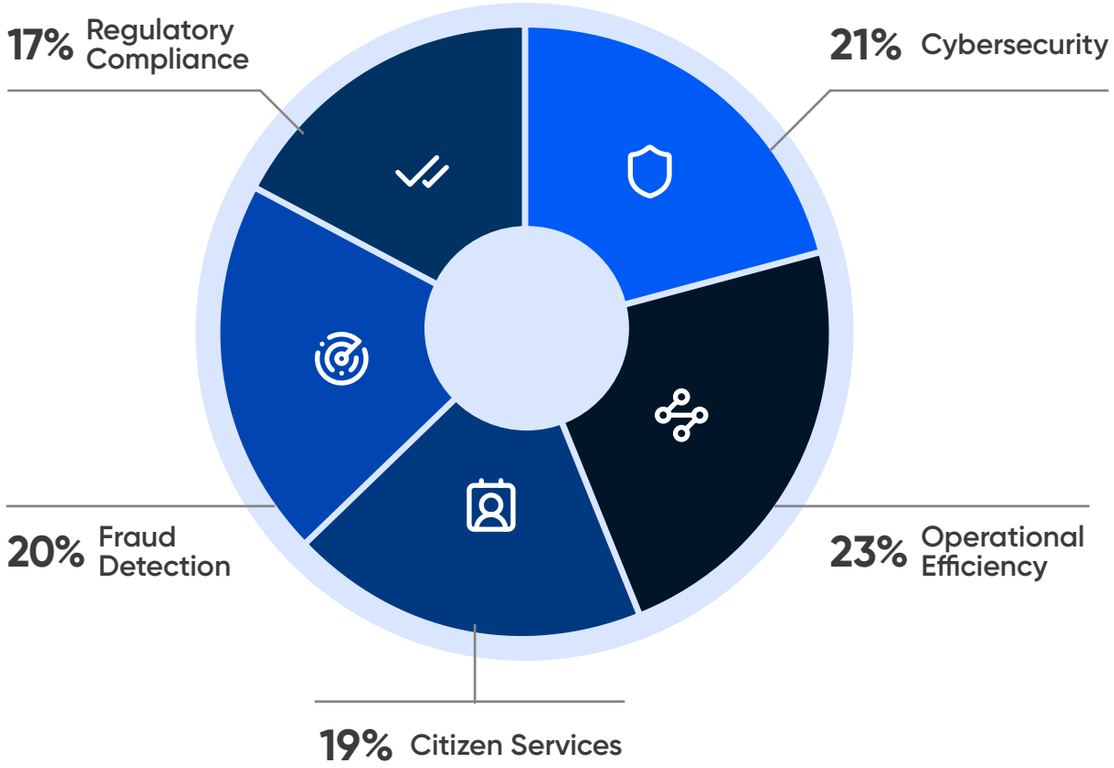
Cory Simpson, CEO, ICIT (Moderator)

John Crossno, Director of Product Management, Rocket Software (Leading interactive discussions)

Mac Gupta, Senior Director, Global Partner Marketing, Rocket Software (Leading interactive discussions)

Steve Roberts, Account Director, MFGS, Inc. (Leading interactive discussions)

AI Use Cases in Government



Road to modernization: From challenges to transformation

Government modernization is not a sprint—it's a mission-aligned evolution. As McCabe highlighted, "The technology really isn't the problem. The problem is we do things a certain way."

Many agencies find themselves digitizing analog processes—an essential first step, but insufficient unless it paves the way toward something faster, more agile, and more valuable. Without process transformation, technology alone delivers little lasting benefit.

Citizen expectations compound these challenges. People interact daily with seamless, AI-powered services in the private sector and expect the same of their government. Yet federal IT leaders must balance agility with security, ensure continuity in hostile environments, and manage vast data ecosystems that stretch across mainframes, cloud platforms, and tactical edge devices.

"Resilience has to stretch into denied environments," McCabe stressed, pointing out that reliance on centralized cloud infrastructure may be untenable in future conflicts. Instead, agencies must architect systems that are locally robust, forward-deployed, and capable of autonomous operation even when disconnected from global networks.

Johnson emphasized that modernization also means right-sizing AI. Smaller, CPU-portable models are increasingly practical for satellites, field systems, and mainframe workloads where GPUs are unavailable.

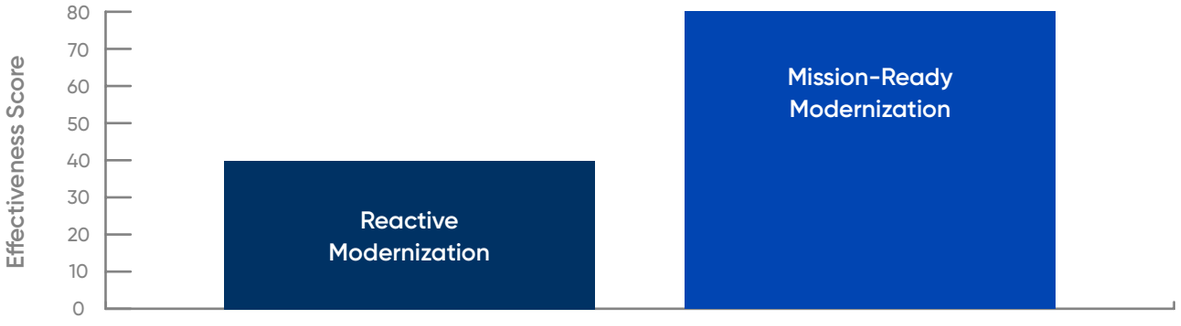
"You get more insights with less data—and at lower cost and latency," Johnson said. This balance of efficiency and reach is especially important for mission-critical operations where bandwidth is constrained. Rocket Software's Enterprise Suite and Data Modernization solutions help agencies extend the life of mission-critical systems while enabling the agility, efficiency, and explainability of data that AI-powered operations demand.

Modernization isn't just about efficiency—it also demands trust.

McCabe underscored the importance of explainable AI: "We want the LLM to be able to come back and explain … 'This is what the machine did, and this is why'." In intelligence operations, black-box models are unacceptable; decisions must be traceable, validated, and defensible.

Hansen added another dimension: AI enables performance-based metric analysis. Rather than reporting after the fact, agencies can use operational data to predict outcomes, foresee disruptions, and respond proactively. This predictive capability can help agencies move from reactive compliance toward proactive mission assurance.

Modernization vs. Mission Alignment



During breakout discussions, Crossno guided attendees toward practical first steps:

- Understand your system architecture.
- Identify mission-critical components.
- Build in resilience.

Start small and improve incrementally, he urged. Hybrid environments, visibility gaps, and orchestration challenges will persist—but they can be mitigated by iterative modernization guided by clear mission priorities.

What agencies should do next: Anchor modernization initiatives in mission outcomes, not technology replacement. Build on existing investments to streamline operations, reduce costs, and sustain continuity while accelerating innovation. Focus on practical steps that move transformation forward without disruption.

Workforce, skills, and cultural barriers

A recurring theme throughout the discussion was the human element. Federal agencies face a shrinking pool of mainframe and legacy system experts at the very moment these systems remain central to mission operations.

Attracting and retaining new talent is difficult when younger professionals are more familiar with modern cloud-native architectures. Training, upskilling, and knowledge transfer are urgent priorities.

Panelists stressed that culture can be as much of a barrier as technology. Many organizations resist change because existing workflows feel familiar, even when they are inefficient. Leaders must actively drive cultural transformation, fostering collaboration between cyber teams, mission owners, and IT staff to ensure modernization efforts stick.

Key Takeaways: Mission-Ready Modernization

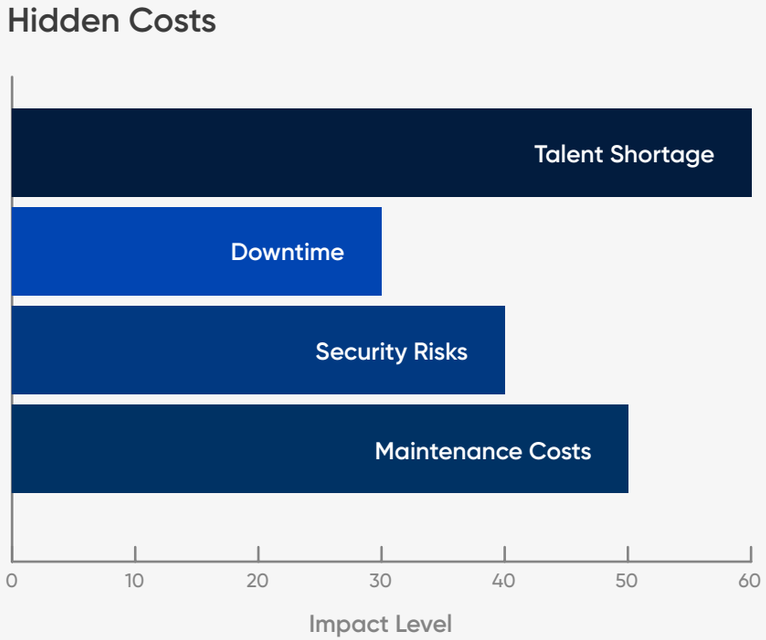
Modernization is cultural, not just technical
Agencies must transform processes and mindsets, not just upgrade tools.

AI must be explainable and efficient
Mission decisions demand transparency, auditability, and performance in constrained environments.

Resilience at the edge is critical
Hybrid approaches ensure continuity even when cloud connectivity is disrupted.

The workforce is the linchpin
Upskilling, knowledge transfer, and cultural change are as urgent as new technologies.

Trusted partnerships accelerate success
Rocket Software and MFGS, Inc. deliver modernization solutions that balance mainframe value, data agility, and AI readiness.



With decades of mainframe expertise, Rocket Software supports agencies in bridging skill gaps – providing tools that make mission-critical systems more accessible to modern developers while maintaining operational resilience.

What agencies should do next: Pair technology modernization with workforce empowerment. Invest in tools, training, and trusted partners that augment limited resources, close the skill gap, and help existing teams do more with less – ensuring mission-critical expertise stays resilient for the long term.

Lessons from the private sector

The private sector has pioneered practices that government can adapt. DevSecOps, continuous integration, and automated testing offer proven pathways to modernization at speed and scale. By embedding security directly into the development pipeline, agencies can reduce vulnerabilities and deploy capabilities faster with fewer resources.

Panelists highlighted that government does not need to reinvent the wheel. Instead, it can translate private sector successes into actionable playbooks, tailoring them to the unique requirements of defense, intelligence, and civilian missions. The key is adaptation, not wholesale adoption—learning from what works while safeguarding national security imperatives.

What agencies should do next: Adapt proven private-sector modernization approaches – like hybrid cloud adoption, DevSecOps, and AI integration – to federal missions. Prioritize incremental progress that improves agility and security with protecting mission-critical systems from risk and disruption.

For more information on Rocket Software and MFGS, Inc, click here: **Federal IT Modernization Solutions | Rocket Software**

ICIT CyberRisk ALLIANCE Rocket software

Conclusion and roadmap

Modernization isn't merely a technology upgrade—it's a cultural and operational shift. Agencies must intentionally reshape processes to prioritize mission resilience, embrace AI that's explainable and efficient, and empower architectures capable of autonomy in the field.

The path forward is clear: build systems that are mission-aligned, digitally agile, and operationally resilient. Invest in the workforce to overcome skills shortages. Translate proven private-sector models into government contexts. Above all, ensure modernization efforts remain laser-focused on enabling the mission. Rocket Software and MFGS, Inc. are committed partners in this journey, delivering solutions that help agencies modernize without disruption and prepare for an AI-enabled future while continuing to unlock the value of their mission-critical investments.

This white paper, grounded in insights from ICIT's April 2025 conference and enriched by the expertise of government and industry leaders, offers both caution and optimism.

The challenges are daunting—but with AI, automation, and a commitment to cultural change, federal agencies can achieve true mission-ready modernization.

Expanding the modernization narrative further, panelists emphasized the critical dimension of citizen trust. Modern services must not only be secure and efficient—they must also be transparent and reliable to build confidence among the populations they serve.

Citizens increasingly expect digital government interactions to mirror the seamlessness of commercial platforms. Failure to deliver undermines public trust and erodes confidence in institutions at a time when cyber adversaries are eager to exploit doubt.

Another issue that emerged was the trade-off between cloud centralization and tactical edge autonomy. While the cloud offers scale and flexibility, reliance on far-off infrastructure may not be practical in contested or disconnected environments.

Panelists pointed to hybrid approaches as essential: leveraging cloud where possible but ensuring mission-critical systems are resilient enough to operate independently at the edge. This balance reduces single points of failure and ensures continuity of operations even in crises.

Finally, security and compliance risks in an AI-driven future cannot be underestimated. Automated decisions must align with established policies, regulatory frameworks, and ethical standards.

Agencies must build oversight into AI governance, ensuring models are not only accurate but also auditable.

Hansen noted, performance-based metrics give leaders better tools to evaluate whether systems truly deliver on their promises—before issues escalate into mission failure.

Taken together, these perspectives underscore that modernization is not one project, but a continuous journey.

By aligning technology with mission outcomes, embedding trust and transparency, and striking the right balance between cloud efficiency and edge resilience, agencies can move beyond incremental upgrades to achieve transformation that endures.

What agencies should do next:

- Chart a modernization roadmap that preserves value from core systems while embracing new technologies like cloud and AI.
- Partner with proven providers who understand federal challenges and can deliver modernization without disruption so you can innovate securely, efficiently, and with mission success in mind.

Acknowledgments

ICIT wishes to thank numerous people without whom the report would not have been possible. In particular, ICIT would be remiss if it did not acknowledge its gratitude to Bianca Andre and Tanner Wilburn. Ms. Andre has a diverse background in legislative affairs, contributing to significant legislation such as the Broadband DATA Act. Mr. Wilburn is a J.D. candidate at the Indiana University Maurer School of Law and a Fellow at Indiana University's Center for Applied Cybersecurity Research.

Copyright

ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank whose mission is modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission.

Founded in late 2014, the Institute's work has earned the trust and respect of the nation's most influential institutions and serves a diverse community of technology, policy, and business leaders. By applying a people-centric lens to critical infrastructure research and decision-making, our work ensures that modernization and security investments have both a lasting and a positive impact on society.

Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses and government agencies on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners—including federal, state, and local government organizations—and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world.

As a privately held U.S. corporation headquartered in the Boston area, Rocket Software maintains centers of excellence strategically located throughout North America, Europe, Asia, and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Follow Rocket Software on LinkedIn and X or visit www.RocketSoftware.com.

CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through its trusted information brands, network of experts, and innovative events it provides cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. CyberRisk Alliance brands include SC Media, the Official Cybersecurity Summits, TechExpo Top Secret, InfoSec World, Identiverse, CyberRisk Collaborative, Security Weekly, ChannelE2E, MSSP Alert, LaunchTech Communications, and Execweb.