CLOUD SAFE TASK FORCE
RECOMMENDATION ROADMAP

Recent attacks on the U.S. government's cloud IT infrastructure, often perpetuated by nation state actors, have resulted in massive data breaches, affecting millions of records while also raising concerns about the use of cloud solutions in national security and other critical government operations. As more and more data migrates to the cloud, the attacks have escalated, raising concerns about deficiencies in cyber resilience and operational hygiene, especially in certification processes and dealing with known vulnerabilities.

In September 2023, four nonprofit corporations—MITRE, the Cloud Security Alliance (CSA), the Advanced Technology Academic Research Center (ATARC), and the IT Acquisition Advisory Council (IT-AAC)—launched the Cloud Safe Task Force to review government cloud infrastructure and to offer solutions to address threats. The Task Force held its inaugural event in December, connecting industry and government participants to discuss policy recommendations to ensure that the nation's critical cloud-hosted digital infrastructure remains secure. This paper summarizes key recommendations these experts identified to improve standards, practices, and policies. The chart to the right summarizes the recommendations from a whole of government perspective.

Current Challenges to Secure Cloud Adoption

Significant opportunities exist to enhance our federal government's cloud computing security. Both government and industry stakeholders shared that:

- Government certification processes take too long and are too costly, and the "costs of entry" are a major barrier to small and medium businesses.
- The reauthorization process for already certified cloud environments is costly and time consuming, and inhibits updating and better securing already certified offerings.
- Reciprocity among security control frameworks in the cloud service industry does not exist.
- There needs to be more confidence and trust in the third-party independent assessment organization evaluations used in certification programs.
- Industry needs incentives to improve transparency (e.g., cloud bills of material, vulnerability disclosure) and operational performance.
- Information sharing of threats and vulnerabilities needs to be enhanced.
- Better metrics are needed, including results from real-time monitoring.
- Automation and the use of artificial intelligence (AI) should be leveraged throughout both the certification and monitoring processes.

Several of these challenges are consistent with the Government Accountability Office's (GAO's) recent report on FedRAMP (Cloud Security: Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed, January 18, 2024, GAO-24-106591).

Recommendation Roadmap for Congress, the White House, Agencies, and Industry

Without a collaborative approach to tackling these improvements to cloud security, our nation will continue to face significant attacks, placing unnecessary risk on our national security and critical government missions. The Task Force recognizes the important work of industry, the Office of Management and Budget (OMB), General Service Administration (GSA), Department of Defense (DoD), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and others to date on providing and securing our government cloud environments. The Task Force offers this recommendation roadmap to Congress, the White House, federal agencies, and industry.

CONGRESS

- Introduce secure cloud adoption legislation that addresses:
  - Shared accountability (incentives for industry to discover, prevent, and disclose threats and vulnerabilities to their systems and services)
  - Greater reciprocity across certification programs, possibly including a national Authorization to Operate (ATO) repository[1]
  - AI-enabled continuous monitoring augmented by routine security testing for improved threat detection
  - Greater automation in certification and incident response
  - Improved metrics
  - Liability protection
  - Enhanced oversight of third-party independent assessment organizations
  - Regulatory harmonization
  - Small and medium business barriers to entry
  - An organization to establish and enforce practices using consistent standards.

[Note: This could be a standalone bill or a major section to the update of the 2014 Federal Information Security Management Act (FISMA).]

- Develop a Cybersecurity Scorecard, with the assistance of the Office of the National Cybersecurity Director and the Federal Chief Information Security Officer, that includes real-time indicators and leverages industry's metrics for cloud security.

EXECUTIVE OFFICE OF THE PRESIDENT (EOP)/OMB

- Update Cloud Smart guidance to Cloud Safe. This should mirror many of the topics addressed in the legislation above and include implementation guidance that includes security practices consistent with the latest administration's proposed approaches (e.g., Zero Trust) and requires NIST to develop interoperability standards for security across multi-cloud environments. This overarching guidance should require other executive branch policy updates, including Federal Information Processing Standards (FIPS) Publication 200, to reflect modern security practices and requirements.
- Enhance cyber metrics to include real-time indicators and leverage industry best practices and existing NIST guidance. These enhanced metrics should clearly include several cloud security metrics and be harmonized with existing cyber metric reporting requirements associated with FISMA and performance.gov.
- Establish a public-private partnership to enhance information sharing that leverages AI-enabled threat detection. This entity would be overseen by the Executive Office of the President (EOP) and would serve as the front door for all industry cybersecurity interactions.

AGENCIES

- Work with Congress, OMB, Cybersecurity and Infrastructure Security Agency (CISA), and NIST to improve continuous monitoring, information sharing, certification programs, and workforce challenges. Collaborate with agency cloud management offices to help close knowledge and process gaps.
- Report Cybersecurity Scorecard and metrics to Congress, OMB, and agency leadership.
- Partner with industry to improve monitoring, testing, automation, and measurement (via the EOP public-private partnership recommended above).

[1] We acknowledge the efforts by the DoD CIO to clarify the relationships between DoD ATOs and FedRAMP in its December 22, 2023, memo: https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf. Such relationships need broader clarification by OMB, as these issues are not unique to DoD.

INDUSTRY

- Ensure that the government receives "innovation and security" updates on pace with updates made to non-government commercial cloud offerings. Government recertification processes cannot be a barrier to timely government updates.
- Work with EOP and Congress to enhance continuous monitoring for improved threat detection through AI enablement and routine security testing, achieve greater automation in certification and incident response, implement the reporting of real-time cybersecurity metrics, improve overall security transparency, and improve the adoption of agile acquisition and management processes for cloud operations.

Conclusion

The Cloud Safe Task Force is engaging with policymakers as they consider tackling these legislative and executive policy enhancements. We have scheduled additional working sessions throughout 2024 and plan to publish detailed papers on these recommendations that will provide specific solutions to better securing our ever-evolving and critically important cloud environments. Our plan is to establish a regular meeting schedule for all stakeholders, and we welcome government and industry participation.

About the Authors

Dave Powner is the Executive Director of MITRE's Center for Data-Driven Policy. He previously led GAO's IT management reviews, working closely with Congress, OMB, and federal chief information officers on IT reform efforts, including the Modernizing Government Technology Act, FITARA, and the FITARA scorecard.

Katy Warren is a Senior Principal and Department Manager in the MITRE Cyber Solutions Center. She has been leading the Cloud Engineering Capability Area and is the principal author of the Enterprise Cloud Adoption Framework, which is used internationally.

Mari Spina is a Senior Principal Cloud Security Engineer in the MITRE Cyber Solutions Innovations Center. She has been leading the MITRE Cloud Security Capability Area since joining MITRE in 2014.

John Weiler is the CEO of the congressionally chartered IT-AAC. He has 40 years of information technology management, solution engineering, and architecture experience covering both the private and public sectors.

John Yeoh is the Global Vice President of Research at the Cloud Security Alliance. He has more than 20 years of experience in research and technology and currently provides executive-level leadership, relationship management, and board strategy development.

Tom Suder is the founder and CEO of ATARC, a professional organization that provides a collaborative forum for government, academia, and industry to resolve emerging technology challenges.

About the Cloud Safe Task Force

The Cloud Safe Task Force—a collaboration between MITRE, the Cloud Security Alliance (CSA), the Advanced Technology Academic Research Center (ATARC), and the IT Acquisition Advisory Council (IT-AAC)—reviews government cloud infrastructure and offers solutions to address the threats.

This collaborative effort aims to inform U.S. government leadership about how best to address concerns around Cloud Ecosystem security in terms of practices, standards, and policies needed to protect U.S. national and industrial assets hosted by U.S. commercial Cloud Service Providers (CSPs).

The desired outcome is improvement across three areas: cybersecurity standards and practices; public sector cybersecurity policy; and governance and oversight.