CLOUD SAFE TASK FORCE
NATIONAL CLOUD CYBER FEED INITIATIVE

The Cloud Safe Task Force recommends establishing a national cyber feed—a public-private collaborative effort for comprehensive situational awareness of cyber threats and responses, fed by real-time security information from major U.S. cloud service providers (CSPs) and used by leading federal cybersecurity organizations including the Office of the National Cyber Director (ONCD), Office of the Federal Chief Information Officer/ Office of Management and Budget (OFCIO/ OMB), Cybersecurity and Infrastructure Security Agency (CISA), Office of the Director of National Intelligence (ODNI), and the United States Cyber Command (USCYBERCOM).

Background

The Cloud Safe Task Force (CSTF) was launched in late 2023 to review national cloud infrastructure and to offer solutions to address threats. In early 2024, the Task Force made its initial recommendations to better secure government cloud offerings. These recommendations included:

- OMB enhancing cyber metrics,
- Agencies improving continuous monitoring, and
- Industry enhancing continuous monitoring, automation, metrics, and transparency.

As U.S. government and critical infrastructure workloads and services have moved to commercial cloud environments, the government has to consider how to effectively manage national security posture. Cloud services provide consistency, redundancy, and rapid transformation that are valuable to ensuring security. In fact, cloud-native approaches to security allow for improved visibility and manageability of risk. Achieving this improved security posture, however, requires adapting to the modern cloud ecosystem and a different approach to cloud security.

This approach includes adoption of new techniques like leveraging application programming interfaces (APIs) to gain insights into service configuration, vulnerabilities, data flows, and other data security–relevant data elements. It requires a constant monitoring of the shared responsibility model inherent in commercial cloud adoption, which dynamically affects the national cyber risk posture. Additionally, the federal government must recognize the critical role CSPs now play in protecting national security and bolstering the federal government's efforts to both deter and defend against cyber criminals and hostile nation-state actors.

Task Force Recommendation to Use Existing CSP Real-Time Monitoring Capabilities

The CSTF met on April 8, 2024, to discuss issues and solutions associated with measuring cloud security, establishing management metrics, and monitoring security for cloud services engaged in the national cyber fight. Three critical observations were made:

1. Highly valuable measures of security can be obtained from passive monitoring of openly available network traffic and web services; it is also critical to leverage cloud APIs to take full advantage of modern cloud platforms.

2. Metrics for measuring security performance should consider cyber resiliency, including risk measurements based on multiple threat vectors, and incident management data such as "time-to-detect," "time-to-respond," and "time-to-recover" for attacks.

3. The visibility vantage point held by key U.S. commercial cloud service providers could be leveraged to improve the U.S. government's ability to detect and coordinate responses to cyber threats. CSP representatives suggested that the government obtain real-time security feeds currently used by the large CSPs to create an integrated, single, national view of our nation's cloud security.

The CSTF is proposing a public-private collaboration between the nation's most prevalent CSPs and government leaders charged with national defense. It is believed that focus should be placed on achieving the ability to collect, aggregate, and incorporate CSP cyber visibility capabilities into national cyber defense. On the government side, suggested participants in this proposed collaboration are ONCD, OFCIO/OMB, ODNI, CISA, and USCYBERCOM. On the industry side, suggested participants in the proposed collaboration are Amazon, Microsoft, Google, Oracle, and IBM. It is imperative that any derived solution must include consideration of capabilities and viewpoints from each of these organizations.

Initial Plan for the National Cloud Cyber Feed Initiative

These U.S. organizations, operating together, hold much of the responsibility for securing the national cyber infrastructure. As much of U.S. information technology (IT) data and systems have moved and continue to migrate to commercial cloud environments, the U.S. government no longer occupies the necessary vantage point from which to measure national IT security and detect and respond to today's national cyber threats.

The CSTF is addressing an increasingly important national infrastructure element that requires coordinated cyber defense. This Cloud Safe National Cloud Feed Initiative seeks to advance the collaboration and policies necessary to deliver real-time cybersecurity monitoring. The initiative is based on the premise that today's dominant U.S.-based CSPs possess the technical means to feed high-value, real-time cybersecurity information to a national-level monitoring dashboard.

The initiative plans to drive the collaboration among government and CSPs necessary to establish both technical and policy agreements for open sharing of critical cybersecurity information. This initiative will be taken up by the CSTF as one of the highest priority objectives for 2024.

This initiative plan aims to enhance cybersecurity information sharing among ONCD, OFCIO/OMB, ODNI, CISA, USCYBERCOM, and major U.S. CSPs, including Google, Amazon Web Services (AWS), Oracle, and Microsoft. The initiative has three main objectives:

- To establish a regular and structured dialogue among the stakeholders to exchange information on the current and emerging cloud security threats, vulnerabilities, incidents, and best practices

- To create a real-time view that compares the different cloud security measures and their effectiveness across the cloud service providers, based on common metrics and standards

- To propose a governance framework that defines the roles, responsibilities, and authorities of this group

Topics to Pursue/Discuss to Better Define/Operationalize This Initiative

- What are the requirements for the National Cloud Cyber Feed initiative? What information needs to be shared?
- What organizations should provide this information? Big 4 or others?
- What federal agency should sponsor it? What governance structure is needed to support it?
- What protections does industry need in order to effectively share?

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 led the Cloud Engineering Capability Area for more than 10 years and is the principal author of the Enterprise Cloud Adoption Framework (ECAF), 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.

John Bergin is the director of the Enterprise Cloud Division at Microsoft. He is engaged across Microsoft's U.S. government deployments focusing on cybersecurity and compliance operations. He joined Microsoft after serving as a deputy assistant secretary of the Army and was a member of the career Senior Executive Service.

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 CSPs.

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