CLOUD SAFE TASK FORCE (CSTF)
NATIONAL CYBER FEED (NCF) IMPLEMENTATION RECOMMENDATIONS

Background

With the rapid expansion of cloud service adoption, commercial U.S. Cloud Service Providers (CSPs) are in a unique position to assess and monitor national cybersecurity risks. The shared responsibility model in cloud computing has positioned U.S. CSPs as key contributors to national cyber defense, often placing them on the front lines of cyber conflict. However, recent high-profile security breaches impacting both U.S. industries and government entities have shaken confidence in cloud services. Addressing these concerns is essential not only to prevent a potential return to traditional datacenter models—where operational and security complexities are heightened—but also to preserve the numerous benefits cloud services provide. These benefits include scalability, cost efficiency, flexibility, and access to advanced security tools. A shift away from cloud services would not only risk losing the innovation, collaboration, and resilience that cloud environments foster but also reintroduce complexities, slower threat detection, and inefficiencies in large-scale cybersecurity management.

To tackle these challenges, the Cloud Safe Task Force (CSTF) was established in September 2023 to develop comprehensive solutions for U.S. cloud security. The Task Force is a collaborative initiative led by MITRE, the Cloud Security Alliance (CSA), the Advanced Technology Academic Research Center (ATARC), and the IT Acquisition Advisory Council (IT-AAC). On July 1, 2024, the CSTF convened a summit to refine its proposal to establish a National Cyber Feed (NCF) to provide a real-time snapshot of cloud security. The discussions focused on the government's need to monitor data and the challenges CSPs face in delivering effective cyber risk and threat intelligence.

U.S. CSPs and third-party risk assessment companies possess world-class capabilities for monitoring risk and tracking adversary activities. However, the CSTF concluded that current data feeds provided by CSPs require improvement to enable real-time threat detection, response, and defense at a national level. In response to feedback from CSP members, the CSTF recommends moving forward with implementation of an NCF. This feed would aggregate monitoring data from U.S. CSPs, providing a real-time view of the national security posture, tracking adversary behavior, and predicting future threats to critical U.S. infrastructure.

National Cyber Feed Concept

In a recent CSTF meeting, CSP members proposed an innovative approach: utilizing the advanced cyber defense dashboards currently deployed by their security operations teams to strengthen national cyber defense efforts. The core idea is to aggregate and anonymize data from these sophisticated dashboards, enabling real-time risk monitoring across national IT infrastructure. This data, when made accessible across various sectors and government agencies, could be used to enhance collective threat intelligence, drive informed policy

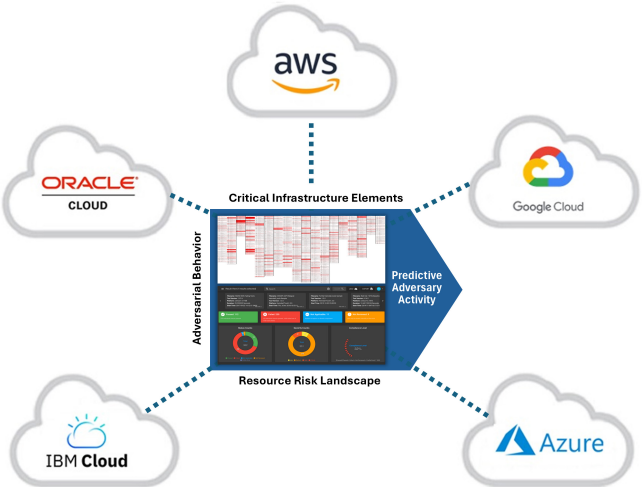

Figure 1

decisions, and enable more proactive cybersecurity measures at the national level. By sharing aggregated data with a broader set of stakeholders, including critical infrastructure operators, public-private partnerships, and cybersecurity coalitions, the NCF concept could transform cybersecurity from a reactive to a preventative stance, ensuring faster and more coordinated responses to emerging threats while maintaining the advantages of cloud-based innovation and security.

CSPs indicated that integrating their data in this manner would pose minimal business risks while providing a critical advantage in tracking and mitigating cybersecurity threats. This approach aligns with the CSTF's vision for the NCF and underscores the potential for substantial advancements in the nation's ability to monitor and respond to cyber threats in real time. By harnessing the data already at CSPs' disposal, the CSTF aims to create a more resilient and proactive cybersecurity posture for the United States.

To advance the National Cyber Feed initiative, the Task Force recommends establishing the NCF as a real-time aggregation of cybersecurity data feeds from major U.S. Cloud Service Providers. This effort would be supported by an independent, non-governmental Third-Party Fusion Organization (I3FO), which would be responsible for integrating, analyzing, and disseminating the data, operating much like existing Information Sharing and Analysis Centers.

The I3FO's role would include safeguarding sensitive and proprietary data contributed by CSPs, ensuring that such information remains protected from public access. It would also interpret the cybersecurity content of the aggregated data and facilitate real-time sharing of desensitized and actionable cyber threat intelligence (CTI). This intelligence would be distributed to key Federal Cyber Authorities including the Office of the National Cyber Director (ONCD), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Cyber Command (USCYBERCOMMAND), Critical Infrastructure Sector Risk Management Agencies (SRMAs), federal agencies, law enforcement, and international partners.

By creating a blueprint for establishing the NCF and empowering the I3FO, the Task Force aims to construct a unified, real-time view of national cybersecurity, enhancing the ability to detect, respond to, and mitigate cyber threats across the entire U.S. digital landscape. This approach leverages the strengths of CSPs and independent oversight, ensuring actionable intelligence reaches those on the front lines of national and international cyber defense.

Data Requirements for the NCF

The CSTF proposes that the initial implementation of the NCF should include data elements aligned to these three security pillars:

1. CSP Infrastructure Security Risk Posture: Real-time assessments of security risks within CSP environments
2. CSP Observed Threat Actor Behavior: Data on adversary activities observed within CSP networks
3. CSP Correlation of Data to U.S. Critical Infrastructure Segments (CIS): Analysis linking security risks and threat behaviors to specific critical infrastructure sectors

This approach allows national cyber defenders to gauge the security posture of different infrastructure segments and provides actionable CTI regarding adversary activities. By associating threat behaviors and security risks with specific CIS, the NCF enables national cyber authorities and SRMA response teams to proactively address threats. Furthermore, these insights may allow for predictions of future adversary behaviors, enhancing the nation's ability to preemptively mitigate cyber risks.

The I3FO will be responsible for fusing data feeds from CSPs, generating near-real-time CTI, and developing forecasts for dissemination to national cybersecurity authorities, federal agencies, SRMAs, CSP members, and partners. It will ensure the protection and anonymization of sensitive CSP and consumer data before distribution. The I3FO will also alert relevant government organizations about emerging threats to enable timely response.

The CTI shared by the I3FO will be non-attributable to specific CSPs or their consumers, focusing on bolstering the cyber risk management and response capabilities of national defenders and SRMAs. By safeguarding data integrity and anonymity, the I3FO will serve as a critical linchpin in the nation's cyber defense strategy, facilitating informed and coordinated action against cyber adversaries.

Organizational Structure of the NCF

The CSTF recommends that the I3FO be an independent, non-governmental, not-for-profit trusted third-party organization. The I3FO will be entrusted to secure the NCF data from misuse and to protect the economic interests of participating CSPs. CISA, having the appropriate charter to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure, is suggested as the government sponsor for the NCF. CISA should assign a government action officer to accept and act on NCF CTI determinations, alerts, and reports.

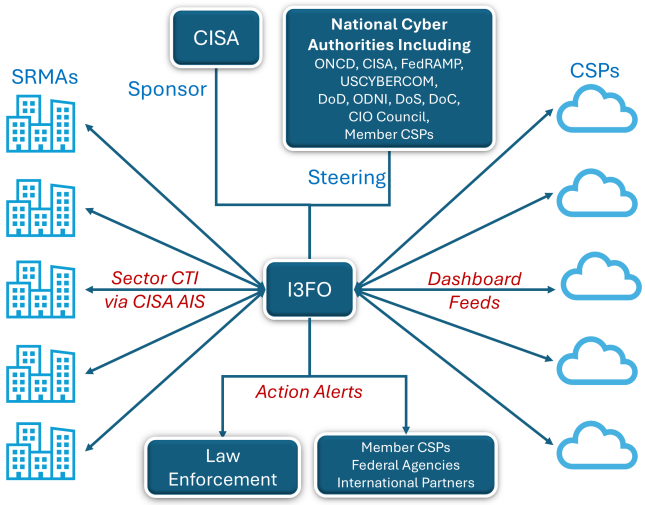

Figure 2

The I3FO should be authorized to enable comprehensive CTI sharing among CSPs, critical infrastructure SRMAs, federal agencies, national cyber authorities, law enforcement, and international partners. It will facilitate cyber-related information sharing through CISA's Automated Indicator Sharing (AIS) service[1] and will play a pivotal role in informing the CISA Joint Cyber Defense Collaborative.

To ensure effective data collection and analysis, the CSTF recommends close collaboration between the I3FO and national cyber authorities including ONCD, CISA, FedRAMP, the Department of Defense (DoD), the Office of the Director of National Intelligence (ODNI), the Department of State (DoS), the Department of Commerce (DoC), and the CIO Council. The Task Force recommends that a dedicated Cyber Coach coordinate with these entities with the I3FO, setting data collection priorities and guiding CSPs in refining their data feed formulation activities.

By establishing the I3FO with strong oversight and clear coordination with national stakeholders, the CSTF aims to enhance the nation's cyber defense capabilities, ensuring real-time, actionable intelligence that supports a resilient and proactive cybersecurity posture.

[1] www.cisa.gov

NCF Implementation Actions

The CSTF recommends a phased approach to implement the National Cyber Feed:

Step 1: Pilot Program in Fiscal Year (FY) 2025
Initiate a pilot program to test and refine the NCF concept, develop requirements, define data confidentiality approaches, and create prototypes for CSP cyber dashboard feeds, I3FO data analysis, CTI sharing, and action alerting capabilities. This pilot should be launched by the Executive Branch—specifically by ONCD or the Office of Management and Budget's Office of the Federal CIO—when the Cloud Smart policy is updated to Cloud Safe, as previously recommended by the CSTF in February 2024. Additionally, Congress is encouraged to mandate this pilot program through the FISMA reauthorization or by introducing it as a standalone bill that updates FedRAMP legislation.

Step 2: Establishment of the NCF Cyber Coach
Create the NCF Cyber Coach role and appoint action officers from key cyber authorities to facilitate collaboration, guide NCF activities, and ensure alignment with national cybersecurity priorities.

Step 3: Full Operational Capability in FY 2026
Based on input from the I3FO, CSPs, and other stakeholders, expand the NCF to full operational status by FY 2026. This expansion will ensure that the NCF can provide timely and actionable cyber threat intelligence to support coordinated national and global cyber defense efforts.

Authors

David Powner, MITRE Center for Data-Driven Policy

Mari Spina, MITRE Secure Enterprise & Cloud Security Engineer

Katy Warren, MITRE Software Solutions & Technologies

Chris Folk, MITRE Cross-Cutting Solutions and Innovation

Reviewers

John Bergin (Microsoft)

Tim Harvey (ATARC)

John Weiler (IT-AAC)

John Yeoh (CSA)

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 threats.

This collaborative effort aims to inform U.S. government leadership about how best to address concerns about 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.

Learn more at www.mitre.org/cloudsafe.