Top Takeaways

The Biden Administration's National Cybersecurity Strategy

The Biden administration's new National Cybersecurity Strategy, released Thursday, seeks to reimagine how the cyberspace is used to achieve U.S. goals, including key shifts in how the U.S. government envisions cyber roles, responsibilities, and resources.

To do this, the Biden Administration strategy introduces two major cybersecurity policy shifts-

- Asking software developers to assume more responsibility for cybersecurity breaches.
- Encouraging long-term financial investment in better cybersecurity practices to slow the chaotic cycle of cyberattacks and ransomware incidents brought on since the COVID-19 pandemic.

During her fireside chat with GovCIO Media and Research's Deputy Editor, Kate Marci, Rajan elaborated upon three key tactics within the new strategy that will be critical to the U.S. cyber success.

LISTEN TO THE FULL FIRESIDE CHAT →

GOVCIO CUSTOMER SPOTLIGHT

Building DHS A Comprehensive Cyber Security Program

The Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) has partnered with GovCIO to apply and improve repeatable information assurance and cybersecurity practices across the DHS's Intelligence Enterprise (DHS IE). We provide a team of 20+ highly-skilled, TS/SCI cleared cyber experts to establish, assess, monitor, and maintain the proper security posture of IT systems and users within its hybrid cloud IT environment.

READ THE FULL CUSTOMER STORY →

> "To talk about open source, we have to talk about the ethos of the system. It's a beautiful concept - the idea that the ideas of one combines the ideas of another [and] makes us greater as whole, that's a fundamentally democratic concept. We're seeing that in Ukraine. We're seeing the open-source community come together to build cryptographic libraries that can help defend against Russian cyber warfare."

-Anjana Rajan, White House Assistant National
Cyber Director for Technology Security

Top Takeaways:

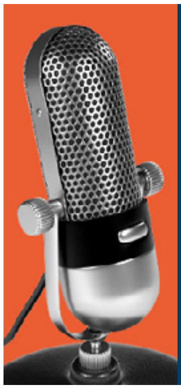
- **Prioritize Open-Source Software Security.** The crux of the new strategy focuses on addressing the challenges faced in securing open-source software, which is ubiquitous to IT and OT systems.
- **Build Upon Zero Trust.** The May 2021 executive order calling on federal agencies to implement zero trust architectures is said to have "set the tone" for this new strategy. As Acting National Cyber Director, Kemba Walden, noted during a presentation hosted by the Center for Strategic and International Studies (CSIS), the goal is for cybersecurity to be "baked in" to software development per a DevSecOps approach, not "bolted on".
- **Build Cybersecurity Awareness.** Federal agencies often talk about building a more cyber-aware culture within their organizations, but all end users of technology need to become more cyber aware.

VIEW GOVCIO MEDIA & RESEARCH'S FULL STRATEGY RECAP →

Transforming Military Ops

GovCIO combines cutting-edge tech and innovative approaches to make today safe and tomorrow smarter.

LEARN MORE →



Get Latest Federal Cyber News with GovCIO Media & Research's CyberCast

A thoughtful perspective on the cybersecurity issues facing industry and government today.

LISTEN NOW →