Aligning with the National Cybersecurity Strategy leveraging Netskope GovCloud

The National Cybersecurity Strategy (NCS), released by The White House in 2023, outlines the strategy and goals that drive a robust, collaborative approach to securing our global digital landscape. To mitigate the ever-mounting risk in both the public and private sectors, The White House has placed cybersecurity as a central tenant to the functioning of the US economy and the strength of its democracy.

As the US president emphasizes at the outset of the NCS, "Digital technologies today touch nearly every aspect of American life," as cybersecurity has become "essential to the basic functioning of our economy" from the operation of our critical infrastructure, data privacy, and national defense.

It is not difficult to extrapolate the outcome given the inflection point we are at as a digital economy. Increased partnerships and data sharing are vital to providing a united front against bad actors that are intent on exploiting our operational dependencies on technology.

> Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense.

National Cybersecurity Strategy, 2023

When it comes to providing this secure foundation for the US Public Sector, commercial solutions have to step up and learn to partner where it makes sense for the American people and Public Sector agencies need to focus more on strategy being what drives compliance and not the other way around.

A true federal partnership for Netskope is more than just delivering a single capability. It's about delivering a set of security and networking capabilities within a high performing cloud-based platform that helps agencies take advantage of economies of scale. Federal agencies need to not only optimize their security, but do it in a way that's both efficient and compliant with federal priorities like TIC 3.0 and Zero Trust Security Architecture while benefiting from shared data feeds.

Netskope's suite of capabilities are uniquely aligned to support the strategic agenda highlighted in the NCS and Netskope's foundational drivers are present throughout to support the strategy:

- Replace legacy tech with agile, cloud-based security stack
- Create a highly-performant cloud infrastructure capable of delivering ROI and increased user experience
- "Better Together" philosophy that drives integration with other tools
- Unparalleled context and visibility giving agencies the control to build a zero trust focused strategy around risk

netskope

Netskope GovCloud enables federal agencies to leverage a cloud-ready networking and security architecture designed to deliver zero trust with multiple types of protection on a FedRAMP High authorized framework. Using Netskope GovCloud, federal government agencies can achieve:

- **Comprehensive protection:** As conditions change and requirements evolve, organizations can deliver new protections by enabling services within Netskope GovCloud. Netskope GovCloud is a fully integrated platform, not a collection of point products, and can be extended to cover a range of threat and data protections.

- **Reduce operating complexity with a single client and single management platform:** Netskope's architecture and Zero Trust Engine leverages a single client for multiple services to reduce the impact on endpoint administration. It uses a single management console with a single policy engine to reduce administrative complexity.

- **Enforces zero trust principles:** Inline with the zero trust requirements in Executive Order 14028, Netskope GovCloud reduces the attack surface area and enforces contextual access controls to dramatically increase the overall integrity of the agency's operating environment.

- **Seamless user experience:** Inline with the approach proposed in NCS, foster undisrupted and secure user experience across the digital ecosystem

"Achieving FedRAMP High authorization for the Netskope GovCloud platform underscores Netskope's continued dedication to helping secure the U.S. federal sector," said Dave Peranich, Netskope President, Go-to-Market. "It is a privilege for Netskope to have such a trusted sponsor and partner in the U.S. Department of Veterans Affairs. As the leading vendor that can offer a comprehensive SSE solution on a single platform with FedRamp High authorization, we remain fully invested in ensuring our platform is the most complete and highest-performing cloud-based solution possible for customers everywhere."

Ultimately, the NCS aims to build cyber resilience through collaboration between stakeholders across the digital ecosystem and further emphasize on long-lasting public-private partnerships. And where this strategy is going to bring the biggest impact is in understanding how to share data securely across users, devices, clouds, and geographic locations..

Through the implementation of this strategy, federal agencies will be better protected through the creation of specific legislation that sets a standard that vendors have to be able to make reality.

As you consider how your current defenses stack up against the ever-changing security landscape and the NCS implementation to come, use the free Netskope SASE Assessment to measure your readiness.

For more information, visit www.netskope.com/solutions/government or download the Netskope GovCloud Solution Brief

Questions?
Contact us at federal@netskope.com.