How Netskope's Capabilities Align with the National Cybersecurity Strategy

The Biden-Harris administration recently released its long-awaited National Cybersecurity Strategy (NCS), intended to tackle the nation's most pressing cybersecurity issues. This strategy outlines the strategy and goals to 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 our economy and the strength of our democracy.

As the 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.

> 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

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. 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 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.

In reviewing the NCS, it was immediately apparent that not only were Netskope's suite of capabilities uniquely aligned to support the strategic agenda but Netskope's foundational drivers are present throughout.:

- 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 strategy around risk

Netskope has spent a decade building on these architectural principles in what has become the most performant security cloud service. This is evident in the way the strategy addresses cloud security, zero trust architecture, data protection, and automation.:

- **Cloud Security:** Netskope helps organizations to secure their cloud environments by providing visibility and control over all cloud services in use, including shadow IT. This ensures that sensitive data is protected, and security policies are enforced across all cloud services.
- **Zero Trust Architecture:** The new national cybersecurity strategy continues the emphasis on agencies adopting a Zero Trust Security Architecture strategy. Netskopes context and visibility into cloud traffic provides the data with which to progress along a ZTA maturity model. Netskope's zero trust network access (ZTNA) solution allows organizations to provide secure access to applications, regardless of whether they are hosted in the cloud or on-premises. Proper application of Zero Trust principles is also a critical step toward Secure Access Service Edge (SASE) architecture.
- **Data Protection:** The protection of sensitive data is a key objective of the new cybersecurity strategy. Using a data protection architecture, agencies can manage risky activities to designated instances even prior to using data loss prevention (DLP). Netskope's DLP capabilities feature AI/ML policies to allow organizations to identify and prevent the unauthorized transmission of sensitive data in the cloud.
- **Automation:** The new cybersecurity strategy aims to promote automation to enhance the speed and effectiveness of security operations. Netskope's Security Operations Center (SOC) automation capabilities provide automated threat detection, remediation, and incident response, allowing security teams to respond to threats quickly and efficiently.

Ultimately, what the federal government is trying to do here is emphasize that just talking about public-private partnerships is not cutting it–this needs to be put into action. And where this strategy is going to bring the biggest impact is in understanding how to share data as it relates to cybersecurity.

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.

Questions?
Contact us at federal@netskope.com.