opentext™ | Cybersecurity

Flash Point Paper

U.S. National Cybersecurity Framework: Cyber Risk and Liability Get a New Paradigm

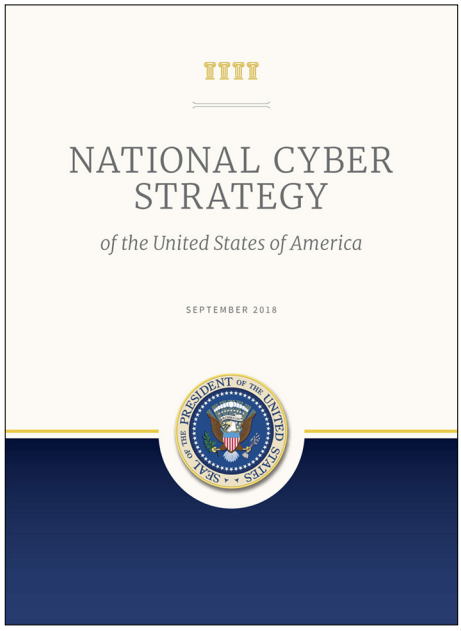
by Stan Wisseman

opentext™ | Cybersecurity

In March 2023, the Biden administration announced a sweeping new National Cybersecurity Strategy (NCS) for the U.S. that I see as a sharp break from past. If fully implemented, the NCS has the potential to change the U.S. cybersecurity posture significantly for the better.

There are five specific pillars identified in the NCS *(see sidebar)*. The NCS builds on cybersecurity efforts from the previous three administrations, as well as on the Executive Orders (EOs) and legislation that has been implemented under President Biden. Of particular note, the NCS seeks to build collaboration and momentum around the foundational direction of EO 14028, "Improving the Nation's Cybersecurity."

However, the NCS also has some major departures from past principles. It calls for a rebalancing of responsibilities, a shift from voluntary measures to regulations, establishes minimum requirements for all critical infrastructure sectors, imposes liability for insecure software products and services, and applies the powers of the entire government to disrupt threat actors. I'll dive into each of these in the sections below.



Rebalancing the Cybersecurity Burden

There was once a time when it was reasonable to expect end users to manage their own cybersecurity. But I think we can all agree that time has passed. Likewise, many small organizations lack sufficient resources to thwart today's cybersecurity threats effectively. The creators of the strategy want to rebalance the responsibility for cybersecurity to be more effective and equitable. The NCS acknowledges that: *"...end users bear too great a burden for mitigating cyber risks. Individuals, small*

The NCS also has some major departures from past principles. It calls for a rebalancing of responsibilities, a shift from voluntary measures to regulations, establishes minimum requirements for all critical infrastructure sectors, imposes liability for insecure software products and services, and applies the powers of the entire government to disrupt threat actors. I'll dive into each of these in the sections below:

- **critical infrastructure protection**
- **disruption of threat actor operations and infrastructure**
- **promoting better security among software vendors and organizations handling individual data**
- **investments in more resilient technologies**
- **international cooperation on cybersecurity**

businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity. A single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens."

In arguing for a rebalancing of the responsibility for cybersecurity, the NCS does not free end users of all security responsibilities. It does, however, indicate that we as a nation must "ask more of the most capable and best-positioned actors" in society. The strategy also recognizes that the U.S. government's role in providing cybersecurity has distinct guardrails. The government's responsibilities include protecting its own systems and networks, ensuring that the private sector does its part to protect itself in cyberspace, and carrying out core governmental functions that support cybersecurity.

Critical Infrastructure Mandates

The critical infrastructure component of the NCS includes a proposal to expand minimum cybersecurity requirements for all operators of critical infrastructure. While voluntary approaches to cybersecurity in the critical infrastructure sectors have produced improvements, the lack of mandatory requirements in some has resulted in inadequate and inconsistent outcomes. The strategy observes: *"Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents."*

Josh Corman, former CISA chief strategist and currently the VP of Cyber Safety Strategy at Claroty, has stated that he believes the administration's choice to make critical infrastructure security a priority in the NCS is an important one. We actually had Josh on as a guest on episode 31 of the Reimagining Cyber podcast where he said that the nation has seen successful cyber disruptions in critical infrastructure during the pandemic. Areas impacted included access to water, food, fuel, and patient care. He characterized them as 'target rich, cyber poor'" industry sectors.

Use of Regulations to Move the Needle

Rather than the traditional, voluntary, "enlightened self-interest" approach to encourage cybersecurity in the private sector, the NCS takes a different approach. The NCS notes that, while the voluntary approach has sometimes improved cybersecurity postures in the private sector, such improvements have not, taken as a whole, been sufficient to meet the national needs for cybersecurity. The approach taken by the NCS is the idea that the strength of cybersecurity cannot be left simply to individual private-sector actors to decide based solely on their business needs, stating: *"In setting cybersecurity regulations for critical infrastructure, regulators are encouraged to drive the adoption of secure-by-design principles, prioritize the availability of essential services, and ensure that systems are designed to fail safely and recover quickly. Regulations will define minimum expected cybersecurity practices or outcomes, but the Administration encourages and will support further effort by entities to exceed these requirements."*

The strategy justifies this approach in the name of public safety and national security needs. That the nation needs a more robust cybersecurity posture than that which would result if left up to these private sector market drivers. The NCS encourages federal regulators to look for opportunities to incentivize all stakeholders to adopt better security practices via tax structures and other mechanisms. With those incentives, they hope to drive security and resiliency by design, strategically coordinate R&D investments into cybersecurity, and promote stewardship of our digital ecosystems.

Rather than create new standards and guidance, the regulations will be based on existing ones such as the NIST Framework for Improving Critical Infrastructure Cybersecurity and CISA's Cybersecurity Performance Goals. In the NCS, the administration commits to improving Federal cybersecurity through long-term efforts to implement a zero-trust architecture strategy and modernize IT and OT infrastructures. Biden's plan is to have the Federal government lead by example.

Liability for Insecure Software Products and Services

In what may be a controversial move, the strategy also puts emphasis on holding software vendors more directly responsible for the security of their technologies. The NCS recognizes explicitly that, left to its own devices, the software market all too often rewards vendors that underinvest in security with greater market share and reduced time-to-market. The strategy states: *"We must begin to shift liability onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers."*

As part of the effort, Biden's administration will work with Congress to try and pass legislation that would prevent software manufacturers and publishers with market power to simply disclaim away liability by contract. The NCS also calls for the development of an adaptable safe harbor framework to shield from liability companies

that securely develop and maintain their software products and services.

Disrupting and Dismantling Threat Actors

The NCS also endorses a highly assertive approach to disrupting threat actors in cyberspace, which I applaud. For example, it says that: *"Disruption campaigns must become so sustained and targeted that criminal cyber activity is rendered unprofitable and foreign government actors engaging in malicious cyber activity no longer see it as an effective means of achieving their goals."*

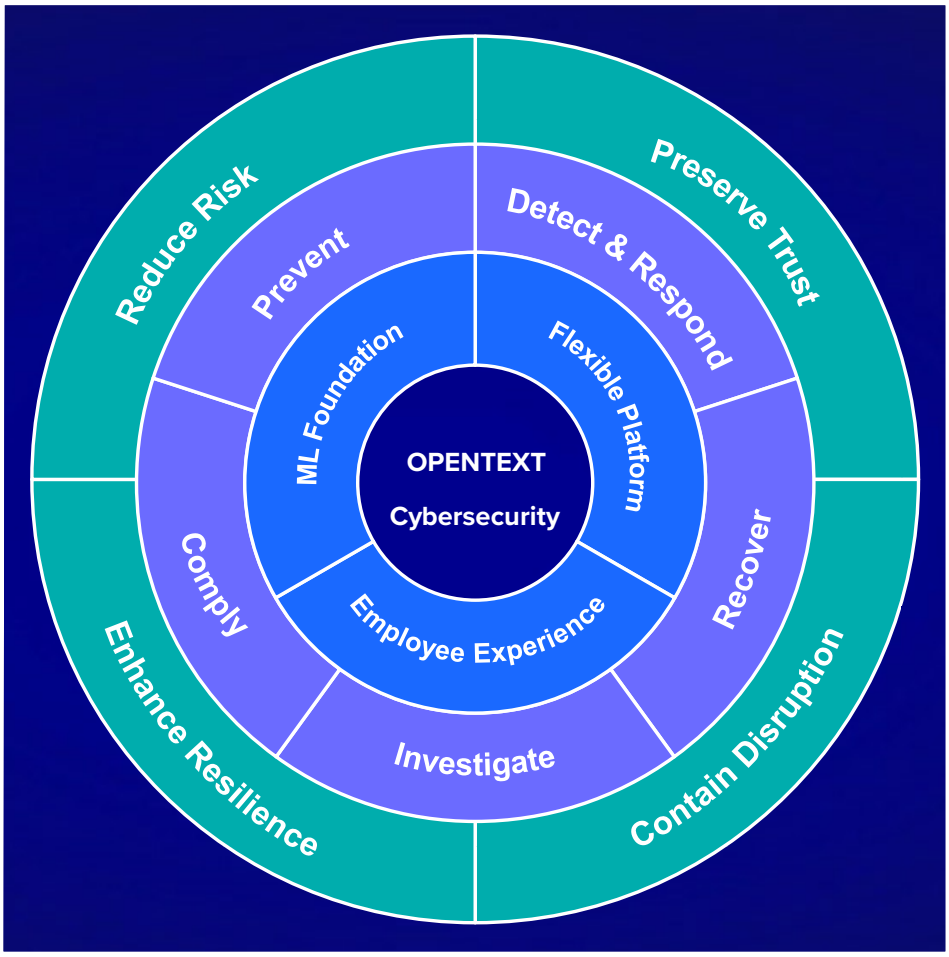
The increased public emphasis on the use of military forces to disrupt threat actors is already apparent in offensive cyber operations taken by U.S. Cyber Command to disrupt the activities of foreign ransomware actors. With the promulgation of strategy, we should expect to see a greater military role in the U.S. cybersecurity posture—one that goes beyond what might be termed "passive defense activities" to active involvement. That's a major shift in policy, but a necessary one given today's threat landscape.

The strategy document is silent on cybersecurity for national security systems, such as those operated by the US Department of Defense and the intelligence community, which makes sense given that it's an unclassified document.

What's Next?

Acting National Cyber Director, Kemba Walden remarked at the NCS's unveiling that the "strategy is only as good as its implementation." The good news is that the strategy is detailed, but not prescriptive, with enough room to innovate. But the NCS still has lots of dependencies and costs associated with it that will take years to implement.

Now comes the need for unified, coordinated, whole-of-community action to bring it to life.



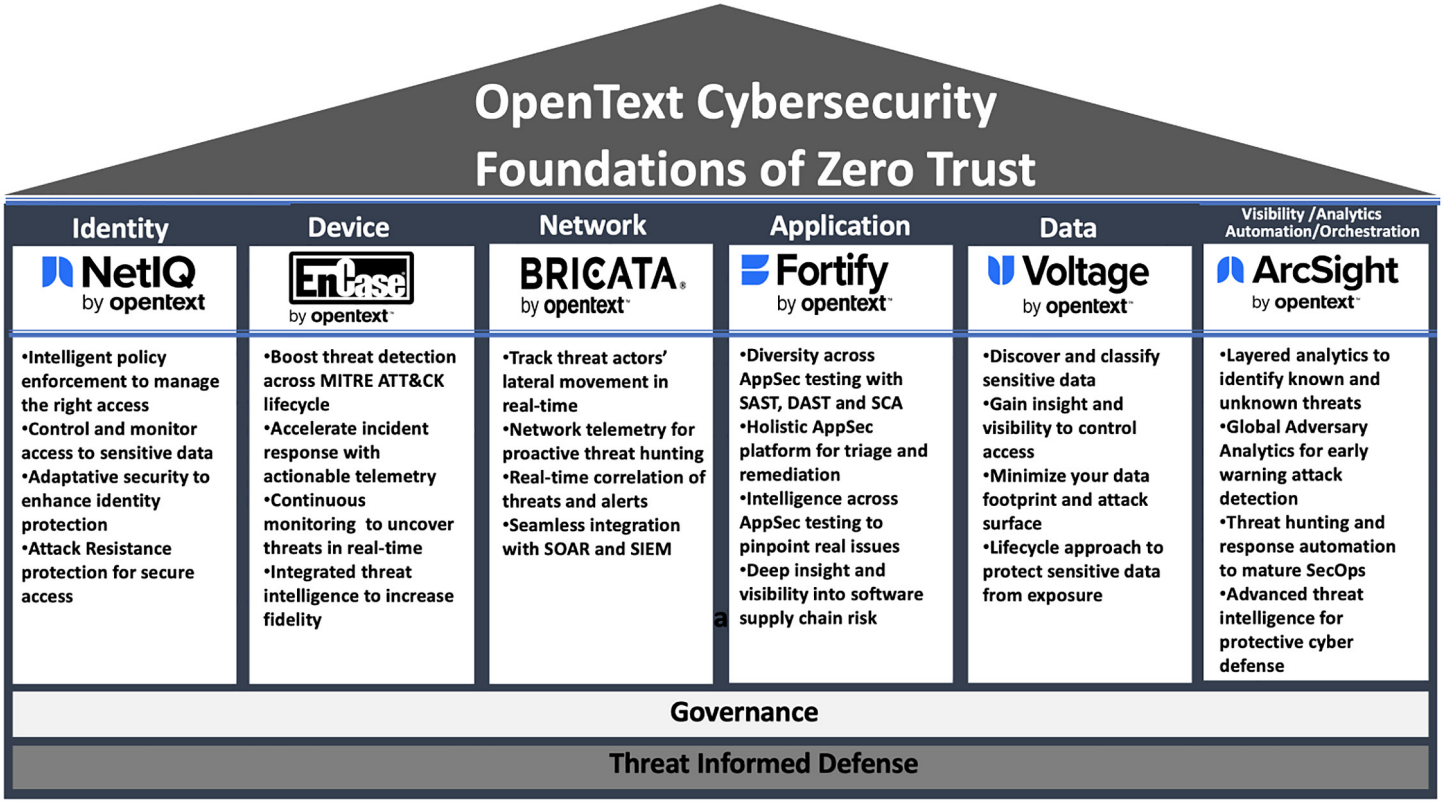
And while this is not the first U.S. federal cybersecurity strategy, it boasts the highest-level agreement and commitment yet from across the executive branch, which bodes well for federal cohesion.

Learn More About How OpenText Cybersecurity is Positioned to Help

The National Cybersecurity Strategy (NCS) endorses zero trust as fundamental in modernizing cyber defense capabilities, emphasizes the importance of cyber resiliency, and amplifies federal guidance outlined in Executive Order 14028.

OpenText Cybersecurity is well positioned to help federal agencies formalize zero trust with breadth and depth to establish data and identity centric context as key components in enforcing zero trust principles with cross-pillar capabilities. OpenText adds intelligence and deep analytics around user behaviors to identify known and unknown threats, as well as provide actionable threat intelligence and early warning capabilities about threat actors to identify gaps and mature zero trust strategies.

Connect with Us
www.CyberRes.com



opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

784-000008-001 | O | 04/23 |