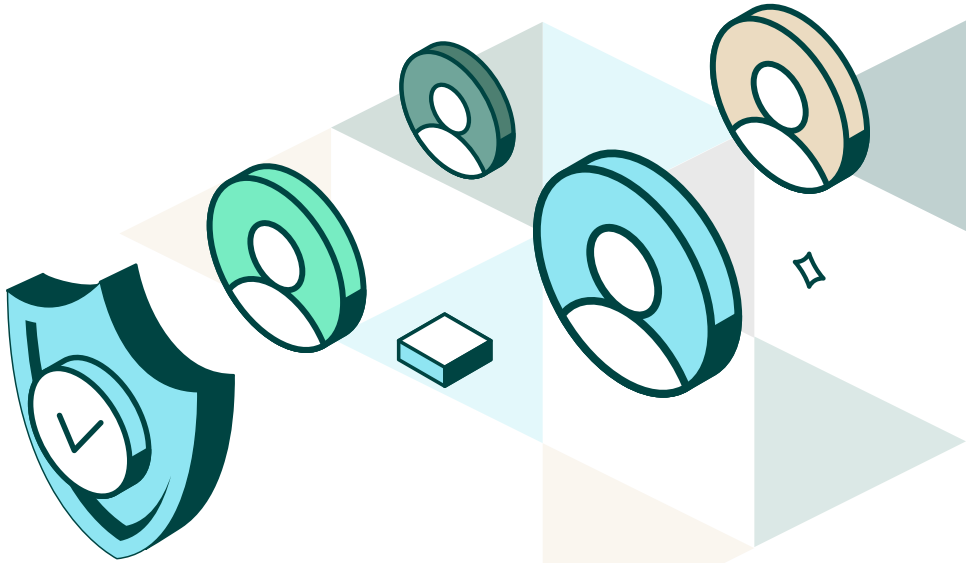
FORTRA™

The White House's 2023 National Cybersecurity Strategy

Fortra's TL;DR

We read it all so you don't have to

Much of the National Cybersecurity Strategy, released by the White House in March, hinges on the concept of shoring up the nation's cybersecurity posture to better protect Americans and the technology they use to communicate.



The strategy, which is full of bold, ambitious ideas and core objectives, serves as a call to action and warns that failing to fortify our defenses and dedicating time and money to strengthen our cybersecurity could harm U.S. interests in the long run.

$65 BILLION
Invested in 2023 National Cybersecurity Strategy

The strategy, which forms a road map for public and private security efforts moving forward, is based around five pillars. Still though, with nearly 40 text-heavy pages, the strategy could take some time to digest.

What's it about in a nutshell? Let's break down the five pillars:

1 Defend Critical Infrastructure

Defend Critical Infrastructure

This pillar is largely about collaboration - rolling out new regulations to secure critical infrastructure, updating incident response plans, and enhancing interdepartmental communication between the Federal Government, private companies, and other allies.

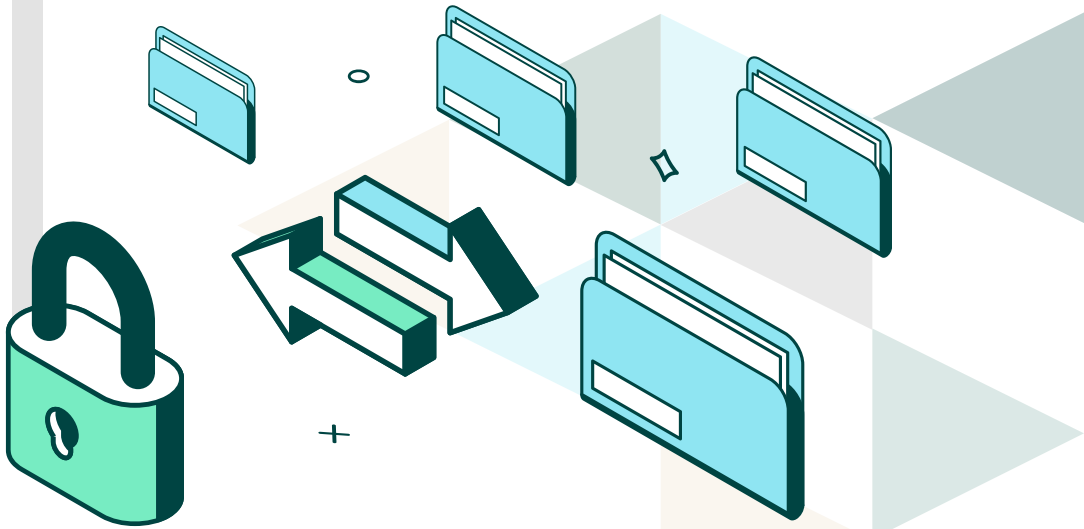
While legislation like the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and groups like the Cyber Safety Review Board (CSRB) have helped satisfy some of this pillar's asks, there's more work to do, including the enactment of further regulations to set baseline cybersecurity requirements to drive better practices at scale and efforts around modernizing and securing agencies and national security systems alike.

2 Disrupt and Dismantle Threat Actors

Disrupt and Dismantle Threat Actors

As the title suggests, this pillar is all about combating and cracking down on malicious hacking campaigns carried out by nation state governments. Whether they've opened the door for ransomware or the theft of sensitive data, these attacks cost the country billions of dollars each year. Defending against these types of attacks has become critical for the government. In the wake of attacks against pipelines, like Colonial Pipeline, water utilities, and hospitals, the U.S. is increasingly viewing attacks against critical infrastructure as a national security threat.

The U.S. also wants more insight from the private sector on how adversaries outside the U.S. operate. This pillar is all about speeding up cyber threat intelligence sharing in order to fight back against cybercrime, ransomware, and any attack that jeopardizes U.S. infrastructure.



3 Shape Market Forces to Drive Security and Resilience

Shape Market Forces to Drive Security and Resilience

This pillar is all about the data and keeping organizations that hold and process that data honest and accountable for their actions. If personal data isn't kept secure, it can have a profound impact on consumer privacy and in turn the digital economy. Bolstering the security of the devices and services that handle this information is a key part of this pillar as well.

One of the more notable components of the strategy, a section that shifts liability onto organizations that fail to secure their software, would require the White House to work with Congress and the private sector to determine what form laws that govern liability for data losses would take. The White House's idea here is that having consequences in place for insecure software could drive the market to produce safe products.

Finding a way to better secure software, with the help of incentive programs, SBOMs (software bill of materials) as well as guidance published by NIST (National Institute of Standards and Technology) will be a focus for the administration moving forward.

4

Invest in a Resilient Future

Invest in a Resilient Future

This pillar prioritizes the nation's future, both through investments in research and development, along with education, in hopes of fostering cybersecurity talent that can, in time, become part of the workforce. The lack of filled cybersecurity positions, along with the lack of diversity in those roles is a problem the country hopes to fix through recruiting, training, and breaking down systemic barriers.

By continuing to research topics like post-quantum computing, artificial intelligence, and biotechnology, the country can both stay ahead of adversaries and ensure that next generation technology stays secure. The federal government is also looking into developing a digital identity ecosystem, something it hopes can thwart fraud and inequity.

300 MILLION
Number of data breach victims stemming from identity theft in 2021

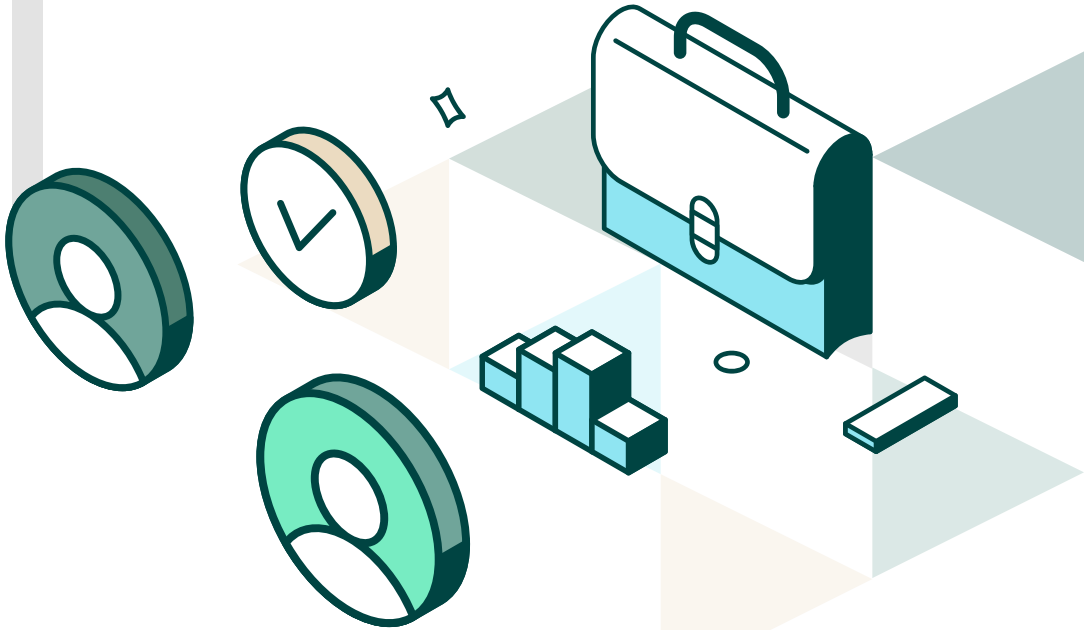
5

Forge International Partnerships to Pursue Shared Goals

Forge International Partnerships to Pursue Shared Goals

The last pillar aims to strengthen partnerships and coalitions to further counter threats. This section, like Pillar One, emphasizes collaboration. By sharing cyber threat information, exchanging model practices, and sector-specific expertise, the United States can stay informed, respond to shifting threats, and preserve diplomacy.

This pillar is especially key for ensuring supply chain integrity, disrupting cybercrime networks and holding those behind them accountable, and advancing U.S. foreign policy and cybersecurity goals on the global stage.



FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 | fta-corp-ebook-0323-rl-as