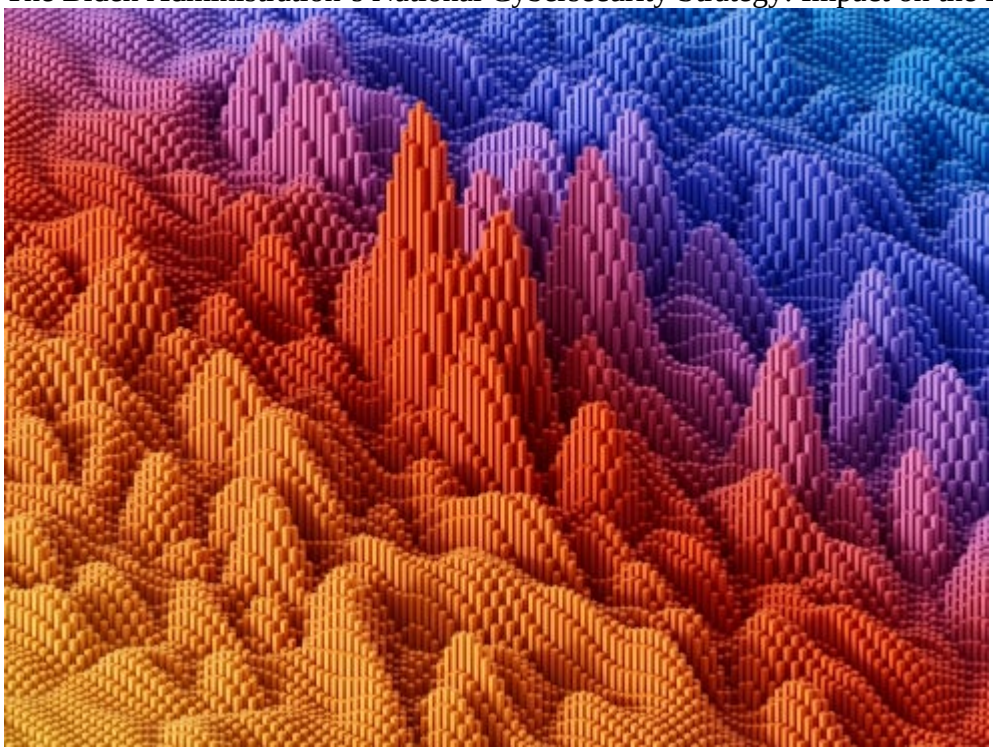
Updates
March 02, 2023
The Biden Administration’s National Cybersecurity Strategy: Impact on the Private Sector



"Continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience."

National Cybersecurity Strategy, March 2023

The Biden Administration released its long-awaited National Cybersecurity Strategy (Strategy) on March 1, 2023. As the quotation above suggests, the days of reporting requirements and facilitating cooperation are over and the U.S. Government will start taking a more active and prescriptive role in private-sector cybersecurity. Industry should expect more incentives, more regulation, and more focus on holding individuals and entities accountable for "left-of-boom" failures to take reasonable security measures.

Increased Regulation

The Strategy heralds the beginning of a long and developing process, but it confirms expectations that cybersecurity mandates will be rolling out. The Strategy specifically refers to the use of existing regulatory authority by the Transportation Security Administration (TSA) and Environmental Protection Agency (EPA) to establish cybersecurity requirements for pipelines, aviation, rail, and water systems. Issuing additional cybersecurity regulations under existing authority is the first concrete step that the Strategy announces. Where the government lacks authority, it will seek it from Congress.

The Strategy further makes clear that cybersecurity regulation will not be limited to industries on the front lines of critical infrastructure. Rather, cloud service providers and other third-party providers should expect greater

engagement and regulation as well.

According to the Strategy, the Administration is committed to developing these regulations in a manner that takes into account the needs and views of industry, including those related to costs and affordability. The Administration also announced its intention for cybersecurity regulations to be deconflicted, harmonized, and streamlined.

The Strategy would not be a federal cybersecurity document if it did not call for public-private collaboration and partnerships. It does not disappoint in that regard. Industry should expect further outreach from federal authorities, sector risk management agencies (SRMAs), information sharing and analysis organizations (ISAOs), information sharing and analysis centers (ISACs), and more. Engagement with such entities will likely provide industry an opportunity to have input into regulatory standards and changes and to enhance their own compliance efforts, in addition to the recognized benefits of sharing cybersecurity threat intelligence and indicators.

Increased Accountability

The Strategy takes the position that those private-sector actors that are best situated to implement cybersecurity best practices lack a market incentive to do so. That lack of incentive leads to inadequate adoption of strong cybersecurity and resilience measures. This, in turn, shifts the security burden to small businesses, end users, and other constituents who lack the resources and sophistication to protect themselves against vulnerabilities built into the systems on which they depend. To correct this market failure, the Administration intends to incentivize security improvements through grants, federal procurement authority, research and development funding, and other measures.

The Administration also intends to push legislative efforts to shift liability for inadequate cybersecurity to providers of software products and services by prohibiting disclaimers of liability and establishing higher standards of care. At the same time, the Strategy calls for a safe harbor framework as a shield against liability.

Another legislative initiative will promote efforts to enhance consumer privacy at the federal level by limiting the collection, retention, use, and disclosure of personal data; protecting particularly sensitive data such as health and location information; and mandating the application of National Institute of Standards and Technology (NIST) security requirements.

Moreover, producers of Internet of Things (IoT) devices, which have been exploited in ways ranging from eavesdropping to co-option into large botnets, appear to have escaped regulatory change for the time being. Instead, federal IoT-related efforts will focus on shifting market forces by labeling IoT products based on their security.

Other Initiatives

The Strategy announces and consolidates other initiatives that have been discussed before, such as fixing Border Gateway Protocol (BGP) vulnerabilities, addressing security problems in the Domain Name System (DNS), and speeding up adoption of Internet Protocol version 6 (IPv6). The federal government's authority in this area is limited, but we should expect to see it attempt to play a stronger coordinating role. We should also anticipate greater investment and involvement in the development and security of forward-looking technologies such as quantum computing, post-quantum encryption and information security, clean energy, and digital identity.

Takeaway

Although the National Cybersecurity Strategy announces many aspirational, long-range goals, recent Biden Administration initiatives demonstrate that the government is prepared to use existing regulatory authority to develop and impose a new generation of cybersecurity rules for private industry. The apparent delay in announcing the Strategy may indicate that a slew of initiatives and rules have been approved for release on a schedule following the Strategy's public rollout. Private industry, particularly critical infrastructure and cloud service providers, should expect more cybersecurity requirements and more opportunity to shape them.

Authors

Explore more in

Privacy & Security | Data Security Counseling and Breach Response | Energy Infrastructure & Clean Technology | Forest Products | Mining | Oil & Gas

Related insights

Update

San Francisco v. EPA: Supreme Court Decides Clean Water Act Permits May Not Include Receiving Water Limits

Update

Your Chance To “Delete” FCC Rules