Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

The National Cybersecurity Strategy—Going Where No Strategy Has Gone Before

Updated July 17, 2023

On March 2, 2023, the Biden Administration released their *National Cybersecurity Strategy* (Strategy). This Strategy follows in a long line of national cybersecurity strategies—including those of the George W. Bush, Obama, and Trump Administrations. Like its predecessors, the Strategy seeks to incentivize adequate and long-term investment in cybersecurity to combat current risks and mitigate future ones. Unlike previous strategies, the Biden Administration's seeks to reshape the landscape of responsibilities in cyberspace—placing a greater obligation on certain types of private sector companies.

This CRS Insight summarizes the Strategy and provides policy context for decisionmakers and considerations relevant to the 118th Congress.

The National Cybersecurity Strategy

In examining the cyberspace threat environment, this Strategy rethinks the understanding of threat actors. First, it states that cybercrime is a national security threat, one which warrants the use of the full array of national powers (i.e., diplomacy, intelligence, military, economic, financial, and informational, in addition to law enforcement capabilities) to combat. The use of non-cyber capabilities to respond to cyberattacks has long been government policy. Then-Vice President Biden implied such a strategy in response to Russia's election interference in 2016. Second, the Strategy states that the People's Republic of China has supplanted the Russian Federation as the primary threat actor to the United States in cyberspace.

To address these threats, the Strategy organizes around five pillars:

- defending critical infrastructure;
- disrupting and dismantling threat actors;
- shaping market forces to drive security and resilience;
- investing in a resilient future; and
- forging international partnerships to pursue shared goals.

Congressional Research Service
https://crsreports.congress.gov
IN12123

These pillars have common objectives that are shared across many strategic documents relating to national cybersecurity, including those from the congressionally authorized Cyberspace Solarium Commission, the executive-directed Commission on Enhancing National Cybersecurity, and the private sector's Cyber Policy Task Force. Such objectives include

- harmonizing regulations;
- collaborating between the public and private sectors;
- integrating cybersecurity centers;
- updating the response plan;
- improving federal cybersecurity;
- coordinating activities to disrupt malicious actors;
- sharing information;
- protecting U.S. cloud computing from abuses;
- disrupting ransomware;
- securing internet-of-things devices;
- incentivizing cybersecurity with grants;
- using federal procurement to improve cybersecurity;
- securing the foundational technologies of the internet;
- spurring federal research in cybersecurity;
- developing quantum resistant encryption;
- ensuring the cybersecurity of the nation's energy systems;
- improving the digital identity system;
- using coalitions to fight cyber threats;
- building partner capacity;
- extending capabilities to allies;
- reinforcing norms of responsible state behavior in cyberspace; and
- securing information and communication technology (ICT) supply chains.

Some of the objectives are new or push existing policy in new directions. These objectives include

- regulating for cybersecurity across critical infrastructure sectors;
- legislating the privacy of data held by stewards;
- holding the final assembler of software responsible for security-by-design;
- leveraging federal funds as a backstop for insurance claims; and
- developing a national cyber workforce strategy.

The document as published lays out a strategic intent for the Administration; the National Cyber Director is responsible for planning and coordinating its implementation. In July 2023, the Administration released the *National Cybersecurity Strategy Implementation Plan*. It follows the strategy's organization of a number of initiatives for each strategic objective, that are organized under pillars. For each initiative, the plan further describes it, assigns a responsible agency, coordinating agencies, and sets a due date.

Considerations for Congress

The Administration has already begun work on advancing much of the Strategy. Congress may choose to exercise oversight of these activities and/or provide additional resources to the Administration in pursuing its objectives.

The five new objectives may require greater investment (and possibly legislative authorization) to accomplish. This affords Congress greater opportunity to debate the merits of each objective and provide direction to agencies.

Two areas that have gained congressional attention are the objectives related to regulation and software liability. In pursuing both of these approaches, the Administration seeks to address an issue with current computing wherein end users bear the burden of software vulnerabilities and their malicious exploitation. The Administration is pursuing a strategic shift of cybersecurity responsibility away from end users towards companies and other parties that are in centralized positions to improve cybersecurity. Previous efforts directed at these parties have sought to encourage responsible behavior with voluntary standards; however, the voluntary nature of such standards led to uneven adoption.

Some organizations have welcomed potential government efforts to clarify the actions that organizations must take for cybersecurity (and the potential liability they might face) in the event of an incident. Uniform expectations and simplified regulatory environments remove certain investment burdens for cybersecurity. However, organizations may also be wary of unintended consequences of government mandates and the impacts those mandates have on their operations. They may also be skeptical that government mandates will be effective at reducing risk or efficiently integrate with business operations. These concerns have already been expressed in the public comments that the Cybersecurity and Infrastructure Security Agency has solicited as they seek to implement a new regulatory authority in the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.