National Cybersecurity Strategy 2023

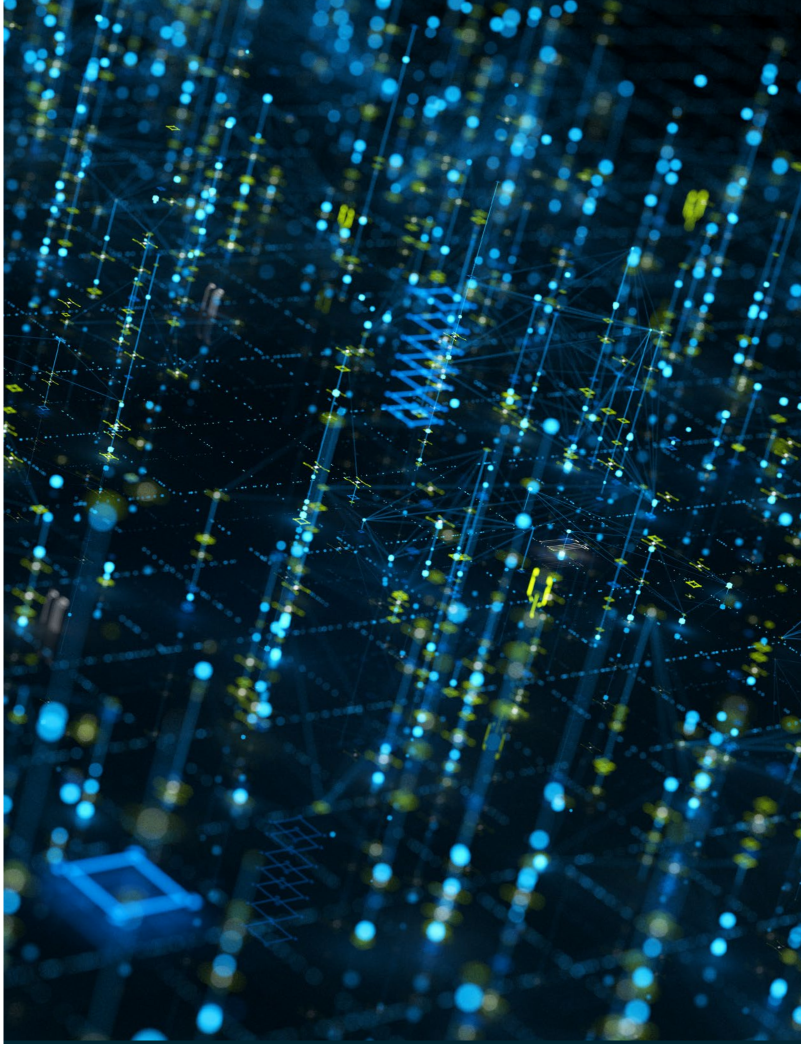
Responding to a rising number of increasingly sophisticated cyber attacks

The Biden administration released the National Cybersecurity Strategy in March 2023 with the goal of achieving a "defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic systemic consequences." [1]

The administration is responding to a rising number of increasingly sophisticated cyber attacks. Our vast digital ecosystem is growing exponentially as more digitally dependent business is conducted over the internet. The list of organizations potentially impacted by increasing threats is endless, incorporating organizations from the local to global level in government, finance, transportation, energy, healthcare, research, and innovation.

In an effort to tackle the cybersecurity challenges across this broad spectrum, the administration lays out five pillars and a series of strategic objectives that build upon the existing cybersecurity Executive Order 14028 policies and initiatives that are being implemented, including modernizing legacy systems through the General Services Administration's Technology Modernization Fund, implementing zero trust architecture (M-22-09), protecting critical infrastructure (NSM-5), securing national security systems (NSM-8), and preparing for quantum computing in the future (NSM-10).

Setting the stage for the current state of cyber adversaries, the strategy identifies four primary countries that present persistent threats to our nation's critical infrastructure and economic prosperity—Russia, China, Russia, Iran, and North Korea. While these countries often have different motives and levels of sophistication, each of them has invested and continues to make significant investments to enhance cyber capabilities. These capabilities can cause disruptions to many essential services and economic activities. The Office of the Director of National Intelligence's 2023 Annual Threat Assessment substantiates the administration's strategic focus on counteracting cyber threats from the below nation states:



The Office of the Director of National Intelligence's 2023 Annual Threat Assessment substantiates the administration's strategic focus on counteracting cyber threats from these nation states:

China

China currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the US homeland, suppression of the free flow of information in cyberspace—such as US web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally.[2]

Russia

The war in the Ukraine was the key factor in Russia's cyber operations prioritization in 2022. Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions.[2]

Iran

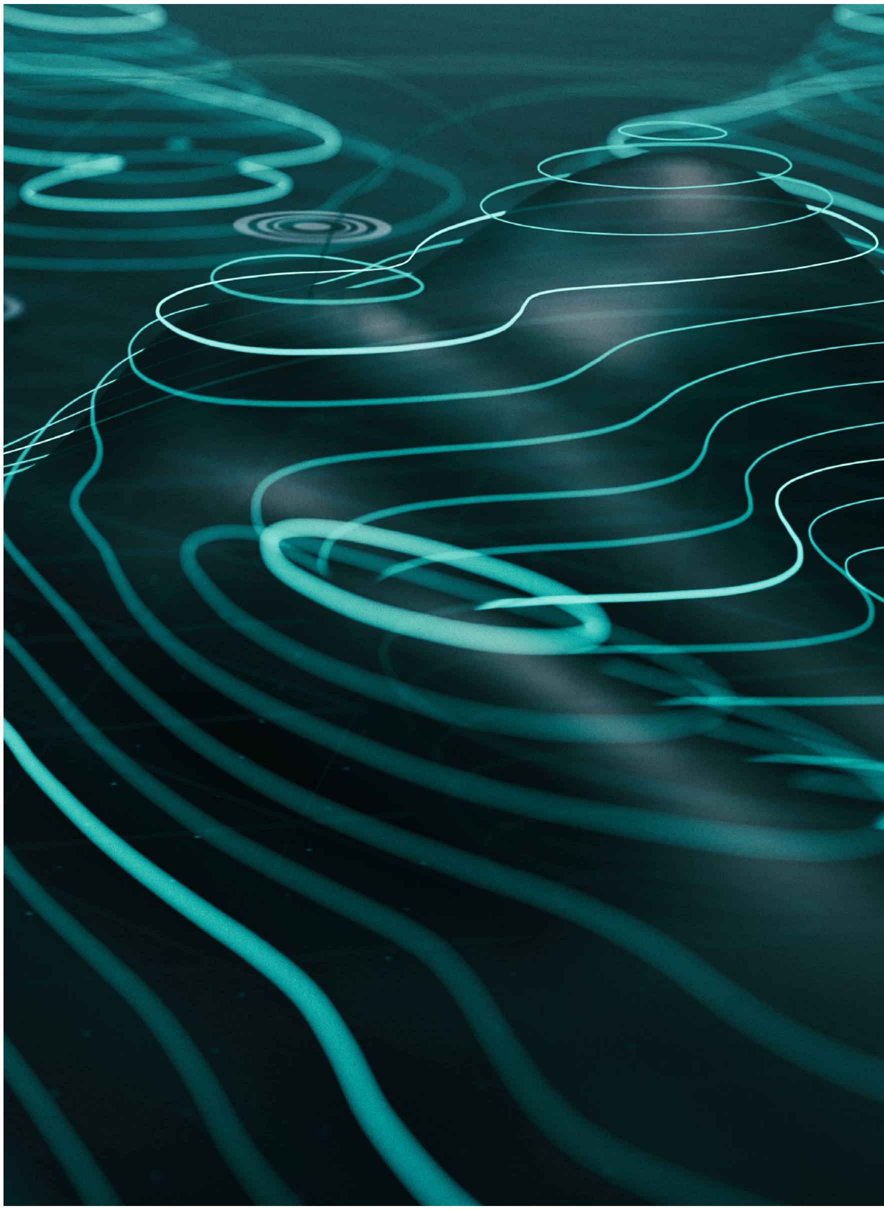
The growing expertise and willingness to conduct aggressive cyber operations make Iran a major threat to the security of the U.S. and allied networks and data. Iran's opportunistic approach to cyberattacks makes critical infrastructure owners in the United States susceptible to being targeted by Tehran, particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains. Recent attacks against Israeli targets show that Iran is more willing than before to target countries with stronger capabilities.[2]

North Korea

The North Korea cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a range of strategic objectives against diverse targets, including a wider target set in the United States.[2]

In the National Cybersecurity strategy, the administration recognizes that the cyber threats to our nation are sophisticated and persistent, and it is very difficult for small companies and organizations to mount a successful defense. The strategy places much greater emphasis on the role of the most capable and best-positioned actors in securing the digital ecosystem. This requires a more prominent role by the Cybersecurity and Infrastructure Security Agency (CISA) as America's cyber defense agency leading the national effort to understand, manage, and reduce risks to the nation's critical infrastructure. It also entails a coordinated effort on the cybersecurity regulatory front to help realize the administration's goal:

- The Office of the National Cyber Director (ONCD) and the Office of Management and Budget (OMB) will lead the administration's efforts to harmonize and streamline new and existing regulations
- The Cyber Incident Reporting Council will "coordinate, deconflict, and harmonize Federal incident reporting requirements" [3]
- CISA will coordinate with Sector Risk Management Agencies (SRMAs) to enable the federal government to scale its coordination with critical infrastructure owners and operators across the United States
- ONCD will lead the administration's efforts to enhance the integration of federal cybersecurity centers, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale
- CISA will lead a process to update the National Cyber Incident Response Plan to strengthen processes, procedures, and systems to unify federal government response to a request for assistance



- OMB and CISA will develop a plan of action to secure the federal civilian executive branch (FCEB) systems through collective operational defense, expanded availability of centralized shared services, and software supply chain risk mitigation
- OMB will lead development of a multi-year life cycle plan to accelerate FCEB technology modernization, periodizing federal efforts on eliminating legacy systems
- The director of the National Security Agency will coordinate with OMB to develop a plan for national security systems at FCEB agencies that ensures implementation of the enhanced cybersecurity requirements of NSM-8

The administration's strategy also shifts the responsibility of protecting data and assuring reliability of critical systems from end users—individuals, small businesses, and state and local governments—to the owners and operators of the systems, and the technology providers that build and service these systems. This has several potential implications, including more direct technical assistance from CISA and other agencies with cyber capabilities to support or help improve the cyber posture of other federal agencies and private, state, and local entities. This fundamental shift in cyberspace defense responsibility amplifies the need for organizations to enhance their cybersecurity capabilities to better protect their critical assets and critical infrastructure. Organizations should take a strategic approach to assessing the current state of their cyber capabilities, identifying gaps, and making targeted investments to strengthen their capabilities.

A well-structured cybersecurity program must enable organizations to accurately identify their critical assets to be prioritized for protection and routinely assess those assets for effective risk mitigation. Guidehouse is well positioned to make individualized current-state assessments of organizations' cybersecurity programs and assist with maturing or developing the programs to balance risk tolerance and enable organizations to achieve their mission or business priorities.

From our perspective, organizations looking to align their cybersecurity efforts to the National Security Strategy 2023 should do so in a prioritized manner. Below are key considerations and actions—laid out in the strategy—that organizations can take to better protect their data and secure their critical infrastructure and critical assets:

- Leveraging the NIST Framework for Improving Critical Infrastructure Cybersecurity and the NIST Cybersecurity Framework along with CISA's guidance and assistance, to assess and mitigate risks to the critical infrastructure

- Modernizing legacy systems to enable adoption of zero trust architecture, or developing a zero-trust roadmap that aligns with the organization's objectives and federal mandates

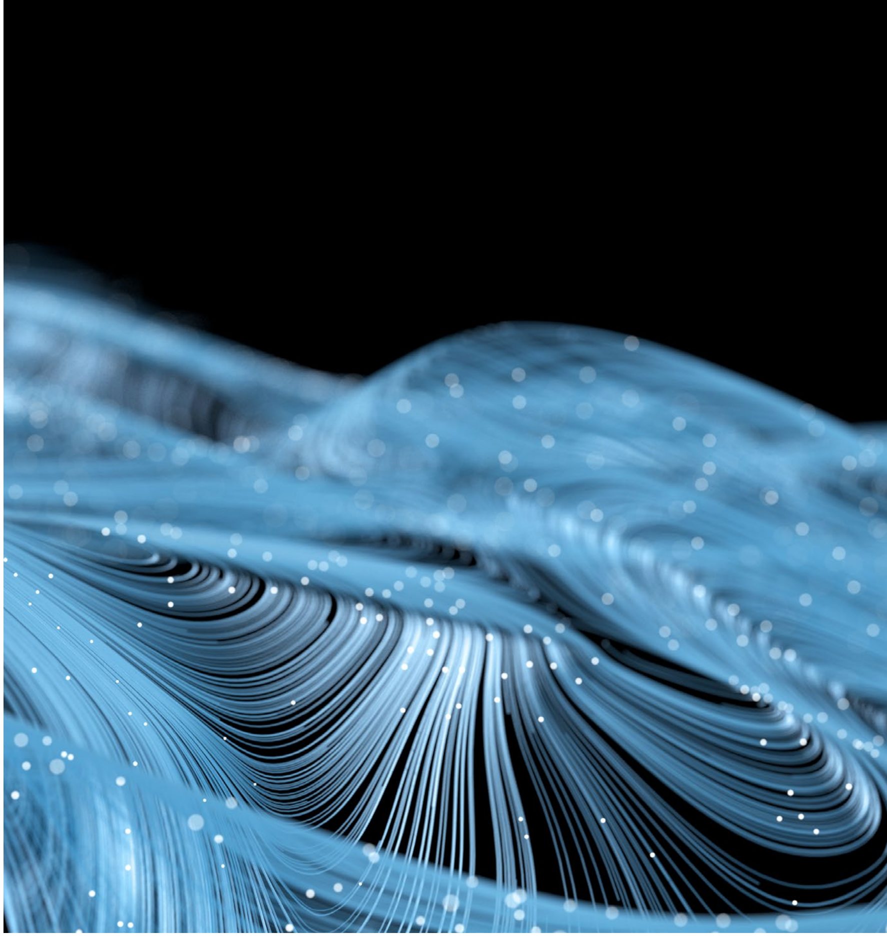
- Applying for and securing federal grants to invest in strengthening cybersecurity programs and capabilities

- Updating incident response plans and processes, conducting tabletop exercises to assess their effectiveness, and establishing a coordination process to connect with CISA's Shields Up program

- Coordinating with CISA to understand the most up-to-date threat intelligence to help prioritize remediation of vulnerabilities to critical assets.

- Developing a supply chain risk management program to understand and manage risks related to third-party suppliers of products and services

Learn more about Guidehouse cybersecurity services



[1] The White House. 2023. "NATIONAL CYBERSECURITY STRATEGY." https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[2] Review of Annual Threat Assessment of the U.S. Intelligence Community. n.d. Office of the Director of National Intelligence. https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[3]"Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA." n.d. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

The White House. 2023. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House. March 2, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

Contacts

Marianne Bailey, Partner
Cybersecurity
mbailey@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

guidehouse.com/services/cybersecurity

@GHtechsolutions linkedin.com/showcase/guidehouse-technology-solutions/

outwit complexity™