The National Cybersecurity Strategy

Policy Analysis

Robert R. Ackerman, Jr.
Founder & Managing Director
AllegisCyber Capital

Richard Stiennon
Chief Research Analyst
IT-Harvest

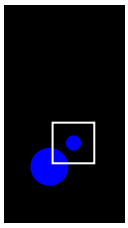
The National Cybersecurity Strategy 2023 Edition

Introduction

After more than a decade the National Cybersecurity Strategy 2023, just released by the White House, is a matured vision of how to address a recognized problem. We are reminded of the old saw “Everyone talks about the weather but nobody does anything about it,” which fits cybersecurity well. National Cyber Policy has been fourteen years in the making, starting with the 60-Day Cyberspace Policy Review by Melissa Hathaway for the Obama White House in 2009.

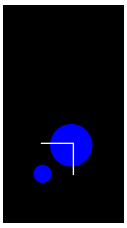
In this analysis we help you understand the 34 page Cybersecurity Strategy, what it does, who it affects, and the opportunities presented.

The document defines five pillars of action that the US Federal government will undertake to address the simultaneous rise of threat actors coupled with a lack of resilience on the part of federal agencies, state and local governments, small businesses, and individuals.



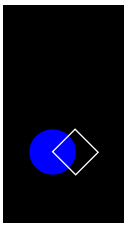
Pillar I.

Defend Critical Infrastructure



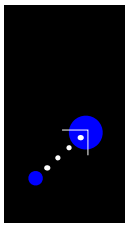
Pillar II.

Disrupt and Dismantle Threat Actors



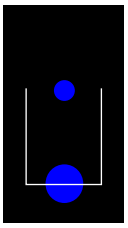
Pillar III.

Shape Market Forces to Drive Security Resilience



Pillar IV.

Invest in a Resilient Future



Pillar V.

Forge International Partnerships to Pursue Shared Goals

Goals

One of the requirements of any strategy is to have clearly defined goals. This strategy does not disappoint. The first goal is broad, but on the mark: To Rebalance the Responsibility to Defend Cyberspace. Today that responsibility falls to the defenders, which is all of us. The second goal is: To Realign Incentives to Favor Long-Term Investments. We believe the five pillars align nicely to further these goals.

The strategy incorporates a not-too-subtle shot across the bows of adversary states. It names—and proceeds to shame—China, Russia, Iran, and North Korea as the principal culprits. Throughout the strategy there are veiled threats of escalation. “The United States will use all instruments of national power to disrupt and dismantle threat actors...” And, “...the United States will employ all elements of national power to counter the threat (of ransomware)....”

Pillar I.

Defend Critical Infrastructure

The definition of critical infrastructure has been expanded greatly since 9/11, while the government has invested massive amounts of money in improving some sectors (highways, bridges) this strategy recognizes the criticality of the software supply chain and the vendors that contribute technology solutions. The effort underway to move chip production back to the United States is a technology driven sector that will come under attack from adversaries and thus proving more justification for a strategy to defend critical infrastructure.

There are five strategic objectives.

1.1 Establish Cybersecurity Requirements to Support National Security and Public Safety

The Administration will seek to use existing regulatory authorizations to impose new requirements for operators of critical infrastructure. Existing guides from CISA and NIST will be expanded. Where gaps exist in those authorizations, the Administration will work with Congress to pass new laws.

1.2 Scale Public-Private Collaboration

CISA is responsible for the overall coordination of public-private collaboration. It works with each Segment Risk Management Agency (SRMA) which in turn works with the Information Sharing and Analysis Organizations (ISAOs) and the Information Sharing and Analysis Centers (ISACs). Technology solutions that enhance the ability to securely share data will be improved and promoted.

1.3 Integrate Federal Cybersecurity Centers

The Office of the National Cyber Director (ONCD) will lead the effort to coordinate and manage all of the various cybersecurity centers.

1.4 Update Federal Incident Response Plans and Processes

CISA will update the National Cyber Incident Response Plan (NCIPR) to provide "who to call" guidance for anyone in industry who is experiencing an incident.

The Administration will work with Congress to codify the Cyber Safety Review Board, created last May to report on major cyber incidents. It will be under DHS.

1.5 Modernize Federal Defenses

This strategic goal is mostly aspirational. By implementing zero trust methodologies the "Federal Government will be a model for private sector emulation."

OPPORTUNITIES

The effort to create better means of sharing intelligence will drive the use of encrypted communications, threat intelligence sharing standards, and the implied key infrastructure needed to secure and track data provenance.

Pillar II.

Disrupt and Dismantle Threat Actors

"The United States will use all instruments of national power to disrupt and dismantle threat actors who...threaten the national security or public safety of the United States."

From Olympic Games to purported support of Ukraine the U.S. has been disrupting threat actors since the Bush administration. It has been successful at indicting nation state actors and dismantling cybercriminal gangs.

This pillar calls for better coordination and expansion of those activities. It serves as a warning to four nations in particular.

2.1 Integrate Federal Disruption Activities

The goal is to dissuade threat actors from engaging in cyber attacks by increasing the pressure. Further coordination is called for. The Department of Defense will update its cyber strategy to clarify the role of US Cyber Command in defending cyberspace.

2.2 Enhance Public-Private Operational Collaboration to Disrupt Adversaries

The 2021 Emotet botnet takedown was an example of public-private coordination to dismantle an attacker group. Industry will be encouraged to expand that cooperation through flexible, virtual "cells" convened to address attacks. These will be supported by secure information sharing infrastructure and expedited "secrecy" authorizations.

2.3 Increase the Speed and Scale of Intelligence Sharing and Victim Notification

More information sharing. This strategic objective promises to streamline the flow of information from Federal agencies to the private sector. This deals with the intelligence gathered by the targets of attacks: IP addresses, indicators of compromise, identity of attackers.

One area that is not addressed in the strategy is the ecosystem of vendors of threat intelligence which make it their business to infiltrate hacker groups, monitor DNS, and collect and correlate intelligence.

2.4 Prevent Abuse of U.S.-Based Infrastructure

The federal Government will work with cloud, email, domain registrars, and hosting providers to make them less available to threat actors for abuse. All service providers must make "reasonable attempts" to secure against abuse and criminal activity.

2.5 Counter Cyber-Crime, Defeat Ransomware

The White House has formed a Counter Ransomware Initiative (CRI) that includes over thirty countries. In January they created an international counter ransomware task force headed up by Australia.

The US will put additional pressure on crypto-exchanges which facilitate ransom payments and discourages the payment of ransoms while still encouraging the reporting of all ransomware incidents.

OPPORTUNITIES

Secure information sharing systems will be needed. Data Rooms may be leveraged to make this possible.

Tools to enable Google, Yahoo!, Microsoft, to recognize when their systems are being abused to spread malware or engage in phishing/scams and shut down abusive accounts. Identity verification vendors could see faster adoption.

The handful of crypto forensics solutions could see increased interest in their products for tracking wallets and ransom payments.

Pillar III.

Shape Market Forces to Drive Security Resilience

There is no question that the next NotPetya could be far more destructive and impact national security. The government will be called on to shore up infrastructure for communications, get the internet back online, and bail out organizations that are critical to recovery, just as it does after an earthquake, hurricane, or financial crisis.

The strategy falls short of addressing a cyber cataclysm, but acknowledges the real possibility by offering to explore a blanket insurance vehicle for cyber incidents. It could have gone much further in its vision to improve resilience. A national disaster recovery plan is called for.

Holding software vendors responsible for security flaws and vulnerabilities in their products has interesting parallels to the early days of rail and air transportation, and certainly medical devices, but the prospect also raises interesting questions:

1. Will a 3rd party application security certification eco-system be created?
2. Will insurance companies step up to underwrite the liability risks?
3. What about “open source”? Who bears the responsibility and takes on the liability?
4. How do you handle legacy code or bespoke systems?
5. Where do you draw the line between vendor responsibility and user liability related to product configuration and operation? Is it a product flaw or pilot error?

3.1 Hold the Stewards of Our Data Accountable

With a nod to the market as the best way to build resilience, the strategy calls for shifting liability to the “stewards of our data” — the product and solution providers that make up that market.

3.2 Drive the Development of Secure IoT Devices

IoT security will be improved by additional Federal grants and purchasing of IoT security solutions. In addition, a system of security labeling will be developed to give consumers the choice to purchase more secure devices, which will incentivize manufacturers to compete on security features.

3.3 Shift Liability for Insecure Software Products and Services

This short section of the strategy is generating the most controversy. For years major technology companies like Microsoft, Google (think Chrome and Android), and Cisco, have only faced reputation and remediation liability for the flaws in their products. There is no arguing that the current cyber threat landscape would be very different if Microsoft in particular had not become ubiquitous in the data center, desktops, and cloud. Future technology companies may fail to innovate as the costs of producing more secure products overwhelm them. Imagine if the nascent AI industry was held liable for flaws in their first products.

3.4 Use Federal Grants and Other Incentives to Build in Security

Federal grant programs will be directed at R&D projects to improve security- and resilience-by design. Organizations will get technical guidance on building security in.

3.5 Leverage Federal Procurement to Improve Accountability

All vendors to the Federal Government will be required to follow and attest to the cybersecurity requirements as they are “strengthened and expanded.” The Civil Cyber-Fraud Initiative (CCFI) leverages the Justice Department to prosecute false claims of being compliant with the regulations.

3.6 Explore a Federal Cyber Insurance Backstop

Instead of emergency bail-outs in the event of a cyber catastrophe the strategy proposes having a backstop already in place.

OPPORTUNITIES

Embedded systems security will get a shot in the arm with an increased focus on producing IoT devices that are secure by design.

Opportunity to participate in the security evaluations that will go into those security labels.

Insurance companies may step in to de-risk product liability for vendors.

Pillar IV.

Invest in a Resilient Future

This pillar is forward looking. It pivots on the governments tools to encourage investment and support standards. It hints at future policies for creating a cyber jobs strategy as well as a digital identity strategy.

4.1 Secure the Technical Foundation of the Internet

The Federal government will support the adoption of critical improvements to the way the internet operates by using secure Border Gateway Protocol and DNSsec. It encourages the switch to IPv6. It will also support standards bodies working on new security standards and protocols.

4.2 Reinvigorate Federal Research and Development for Cybersecurity

Federal investment vehicles, purchasing power, and regulations will be focused on key technology areas like computing, quantum information systems, artificial intelligence, biotechnology and clean energy.

4.3 Prepare for Our Post-Quantum Future

While supporting the development of quantum computing the Federal government will simultaneously work to reduce the threat quantum computing poses to our encryption infrastructure.

4.4 Secure Our Clean Energy Future

The large investments the US is making in renewable energy and infrastructure will be taken advantage of to ensure that cybersecurity is built into these systems as they are designed and deployed.

4.5 Support the Development of A Digital Identity Ecosystem

Enhancing the use of strong identities, validating them, and protecting them, could be transformational. This objective outlines all of the dangers to privacy and security that have to be surmounted in rolling out digital identities.

4.6 Develop a National Strategy to Strengthen Our Cyber Workforce

Mostly aspirational, this objective seeks to guide the Federal government's efforts to train and certify cyber workers while being inclusive. Not a new WPA.

OPPORTUNITIES

Encryption and key management will be important components of a post-quantum world. Expect large investments from the US.

Digital identity providers and Identity Rights Management solutions will be well positioned to take advantage of a renewed focus on identity.

Secure BGP, DNS, and IPv6, are all areas that should get a boost from this strategy

Pillar V.

Forge International Partnerships to Pursue Shared Goals

This pillar is primarily focused on diplomatic efforts to take the lead in guiding international norms of behavior and enforcing them.

5.1 Build Coalitions to Counter Threats to Our Digital Ecosystem

An acknowledgement that most attacks against US infrastructure originate from foreign actors and thus the importance of international cooperation.

5.2 Strengthen International Partner Capacity

DoJ will work on prosecuting cybercrime internationally. DoD will work with other militaries to assist and support. The State Department will work on building coalitions to improve cybersecurity resilience for all democratic states.

5.3 Expand U.S. Ability to Assist U.S. Allies and Partners

The Administration will create policies to determine when the United States can and should provide support to countries that come under attack. It cites the NATO effort to build a virtual incident support capability as an example.

5.4 Build Coalitions to Reinforce Global Norms of Responsible State Behavior

To constrain US adversaries and counter malicious activity the US will work with its partners to combine condemnations with the "imposition of meaningful consequences."

5.5 Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services

A far reaching collection of activities to secure the technology supply chain by pushing sourcing to trusted countries and ensuring that components move through trusted countries.

OPPORTUNITIES

NGOs, think tanks, and policy organizations, will have opportunities to engage with the Federal government on these programs.

Summary

It takes massive effort to get a heavy object moving, but once started it tends to keep rolling. After eighteen years of cyber strategies across five administrations this National Cybersecurity Strategy is being met with grudging praise by most commenters. It builds on previous Executive Orders and brings together the myriad working groups, departments, and agencies that have been formed in response to continuous cyber attacks that threaten national security. It will be changed and added to by this and future administrations.

The strategy, put into action, will start to finally have an impact. The Federal government will become better at defending itself, while assisting states and operators of critical infrastructure.

Opportunities abound, as listed above, to participate. There are commercial opportunities at many levels. Vendors developing identity and encryption solutions will enjoy the tail winds. If dismantling and disruption activities are carried out at the proposed level cyber criminals may be dissuaded from pursuing future attacks.

Many have been frustrated over the decades with the slow government response. Now is the time to support this new National Strategy and look for ways to participate in its execution. While the cybersecurity market is in its early days of growth, the realization of the existential risk to the global digital economy posed by cyber threats, is mobilizing government, industry, operators of critical infrastructure and essential services, and cyber innovators to envision and map an actionable path to a more secure digital future.

AllegisCyber Capital is the market's pioneer in focused cybersecurity investing. With a 20+ history in early-stage cybersecurity investing, AllegisCyber was the world's first dedicated cyber venture firm and raised the market's first dedicated cyber venture funds. AllegisCyber engages with entrepreneurial teams at the series-A to series-C stage of development. As an early-stage investor, AllegisCyber focuses on "proving" technical efficacy, market viability, and commercial scaling of disruptive early-stage cyber companies. Leveraging extensive operating backgrounds and more than 75 years of venture capital company building experience, AllegisCyber works with companies and their management teams to identify and build the next generation of cyber market leaders. AllegisCyber-backed unicorns include Dragos, Shape Security, SYNACK and Signifyd.

For more insights and cyber industry news visit us at https://allegiscyber.com/ or follow us on Linkedin.