President Trump's

CYBER STRATEGY

for America

MARCH 2026

MICROSOFT EXHIBIT 1031
Microsoft v. Qomplx
IPR2026-00183

THE WHITE HOUSE

WASHINGTON

Over the past year, the United States has shown the entire world that we have the most powerful, sophisticated, and technologically advanced military on earth—and it is not even close. This includes not only our overwhelming conventional military strength, but also our unparalleled non-kinetic powers.

The National Cyber Strategy outlines my priorities for ensuring that America remains unrivaled in cyberspace. It calls for unprecedented coordination across government and the private sector to invest in the best technologies and continue world-class innovation, and to make the most of America's cyber capabilities for both offensive and defensive missions.

Our cyber tools and operators are the best in the world—and we are empowering them to defend America by disrupting and disorienting our adversaries, and denying them a safe haven. The United States has capabilities that the rest of the world can only begin to imagine. Our warriors in cyberspace are working everyday to ensure that anyone who would seek to harm America will pay the steepest and most terrible price.

This strategy is about defending the safety, security, and prosperity of the American People. As we approach the 250th anniversary of American Independence, the strategy laid out in this document will help ensure that America remains the strongest, freest, and greatest country in the history of the world, long into the future. American Power will finally stand up in cyberspace.

Cyberspace was born in America. American talent, innovation, research, and powerful government capabilities combined to create a dynamic, thriving, digital world that every American relies on for information, economic opportunity, and our basic way of life. Indeed, the cyber domain is key to President Trump's actions to ensure America leads the world in finance, innovation and emerging technology, military power, and manufacturing.

Freedom and safety in cyberspace, however, cannot be taken for granted. Adversaries and cybercriminals exploit cyberspace to advance authoritarianism, suppress democracy, and undermine our national and economic security.

Unlike other Administrations, the Trump Administration will not tinker at the edges and apply partial measures and ambiguous strategies that neglect the growing number and severity of cyber threats. President Trump will continue to address threats in cyberspace directly.

America enjoys unrivalled technological and economic innovation, unmatched military power, and a society devoted to free and open expression. Every American should take practical steps to protect themselves and their families in cyberspace, but America's citizens do not stand alone. President Trump has demonstrated time and again that he is determined to make Americans secure and prosperous by harnessing all of our comparative advantages. This strategy is a continuation of President Trump's actions, and directly supports the National Security Strategy by putting America first in cyberspace.

Our adversaries and cyber criminals target our families, neighbors, small businesses, farmers, first responders, patients, and senior citizens in cyberspace. They disrupt critical services like healthcare, banking, food supply, and water treatment. They impose tremendous costs on our economy and make everyday goods less affordable.

President Trump's actions, however, send a clear message: we will act to defend our interests in cyberspace. Whether destroying online scammers' networks and seizing $15 billion of their stolen money, supporting a globe-spanning operation to obliterate Iran's nuclear infrastructure, or leaving our adversaries blind and uncomprehending during a flawless military operation to bring international narco-terrorist Nicolas Maduro to justice, adversaries are on notice that America's cyber operators and tools are the best in the world and can be swiftly and effectively deployed to defend America's interests.

Americans re-elected President Trump to put America first. This strategy communicates the Trump Administration's cyber vision and approach to the American people, to Congress, to our partners in industry and allies across the globe—and also to adversaries. It explains the Administration's priorities, summarized in six policy pillars, which will guide action and resourcing through the follow-on policy vehicles. This strategy builds on President Trump's actions to date, and requires a level of coordination, commitment, and political will never before marshalled against cyber threats. President Trump's leadership has created a new era in cyberspace.

Moving Forward

Our resolve is absolute. We will act swiftly, deliberately, and proactively to disable cyber threats to America. We will not confine our responses to the "cyber" realm. We will undertake an unprecedented effort, operating in a coordinated and sustained fashion across the U.S. government. Working with allies across the globe, we will promote U.S. interests and security. We will fight the curtailment of free speech. We will outcompete adversaries who sell "low cost" AI and digital technologies that carry embedded censorship, surveillance, and ideological bias. We will partner closely with industry and academia, at the speed and scale commensurate with the threats we face, and in accordance with our values.

President Trump has made targeting Americans a hazardous business. Our adversaries have and will increasingly feel the consequences of their actions; we will dismantle networks, pursue hackers and spies, and sanction lawless foreign hacking companies. We will unveil and embarrass online espionage, destructive propaganda and influence operations, and cultural subversion.

By disrupting adversaries' cyber campaigns, and making our networks more defensible and resilient, we will unleash innovation, accelerate economic growth, and secure American technology dominance. We will remove burdensome, ineffective regulations so that our industry partners innovate quickly in emerging technologies. Partners in the private sector must be able to respond and recover quickly to ensure continuity of the American economy. We will defend our federal systems, critical infrastructure, and supply chains by putting security at the foundation of innovation. We will modernize our information systems so that old infrastructure does not choke innovation. We will engage internationally through diplomacy, commerce, and operations to ensure norms and standards reflect our values. We will leverage the immense talents and ingenuity of our private sector research base. We will establish a new level of relationship between the public and private sectors to defend America in peace and war.

Pillars of Action

Six Policy Pillars underpin this strategy and will guide implementation and measures for success.

1. Shape Adversary Behavior

American citizens, companies, and our allies should not have to fend off sophisticated military, intelligence, and criminal adversaries in cyberspace alone. We will deploy the full suite of U.S. government defensive and offensive cyber operations. We will unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities. We must detect, confront, and defeat cyber adversaries before they breach our networks and systems. We will erode their capacity and capabilities, and use all instruments of national power to raise the costs for their aggression. We will counter the spread of the surveillance state and authoritarian technologies that monitor and repress citizens. Cybercrime and intellectual property theft are some of the greatest threats to global economies. We will uproot criminal infrastructure

and deny financial exit and safe haven. Defending cyberspace and safeguarding freedom is a collective effort—the distribution of cost and responsibility must be fair across the U.S. and allies who share our democratic values. We will work together to create real risk for adversaries who seek to harm us, and impose consequences on those who do act against us.

2. *Promote Common Sense Regulation*

Cyber defense should not be reduced to a costly checklist that delays preparedness, action, and response. We will streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally. We will streamline data and cybersecurity regulations to ensure that the private sector has the agility necessary to keep pace with rapidly evolving threats. We will emphasize the right to privacy for Americans and American data.

3. *Modernize and Secure Federal Government Networks*

We will accelerate the modernization, defensibility, and resilience of federal information systems by implementing cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition. We will work to elevate the importance of cyber in government leadership and in the board room. We will use the best technologies and teams to constantly test and hunt for malicious actors on federal networks. We will prioritize the security and resilience of the National Security Systems that underpin our military, intelligence, and civilian enterprises. We will work to adopt AI-powered cybersecurity solutions to defend federal networks and deter intrusions at scale. Working across the government to modernize and create competitive procurement processes, we will remove barriers to entry so that the government can buy and use the best technology.

4. *Secure Critical Infrastructure*

We will identify, prioritize, and harden America's critical infrastructure and secure its supply chains, including defense critical infrastructure and adjacent vendors, private companies, networks, and services—such as the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals—securing information and operational technology supply chains. We must move away from adversary vendors and products, promoting and employing U.S. technologies. We will deny our adversaries initial access, and in the event of an incident, we must be able to recover quickly. We will galvanize the role of state, local, Tribal, and territorial authorities as a complement to—not a substitute for—our national cybersecurity efforts.

5. Sustain Superiority in Critical and Emerging Technologies

Securing American innovation and protecting our national intellectual advantage will be paramount. We will build secure technologies and supply chains that protect user privacy from design to deployment, including supporting the security of cryptocurrencies and blockchain technologies. We will promote the adoption of post-quantum cryptography and secure quantum computing.

And we will secure the AI technology stack—including our data centers—and promote innovation in AI security. We will swiftly implement AI-enabled cyber tools to detect, divert, and deceive threat actors. We will rapidly adopt and promote agentic AI in ways that securely scale network defense and disruption. Through cyber diplomacy, we will ensure that AI—particularly generative AI and agentic AI—advances innovation and global stability. We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and frustrate the spread of foreign AI platforms that censor, surveil, and mislead their users.

6. Build Talent and Capacity

President Trump has called America's cyber workforce a strategic asset that "protects the American people, the homeland, and the American way of life." It is an asset worthy of great investment and essential to our nation's economic prosperity and security. We need a pipeline that develops and shares talent. It must be pragmatic and accessible—reconciling and taking advantage of existing avenues within academia, vocational and technical schools, corporations, and venture capital opportunities—to educate and train our existing cyber workforce across industries and occupations, and to recruit the next generation to design and deploy exquisite cyber technologies and solutions. We will eliminate roadblocks that prevent industry, academia, government, and the military from aligning incentives and building a highly skilled cyber workforce. We will harness the existing resources, authorities, talents, and ingenuity that make America great.

Conclusion

This strategy makes clear the course President Trump has pursued in cyberspace, and the direction the U.S. government will pursue with increasing impact. President Trump has acted to ensure that Americans—especially future generations—will have a strong country where they are secure and defended, and a future defined by individual freedom, economic prosperity, and opportunity. President Trump will continue showing those who harm our interests and attack our values in cyberspace place themselves at risk.

THE WHITE HOUSE

WASHINGTON