# A Strategic Intent Statement for the Office of the National Cyber Director

THE WHITE HOUSE
WASHINGTON

# Table of Contents

# A Strategic Intent Statement for the Office of the National Cyber Director

## The Vision

Everyone deserves the full benefits of participation in our interconnected society, an equal share in the prosperity of our digital economy, and freedom from fear of online coercion or repression.

This is not our reality today – but it can be.

Recent history has forced us to predominantly consider cybersecurity in negative terms – which hackers must be stopped, vulnerabilities patched, and activities condemned, sanctioned, or disrupted. It is easy to forget that cyberspace was originally built to enrich our lives. Digital connectivity is not some occasionally-destructive force of nature to be dispassionately tracked and mitigated, but a transformational tool to be wielded in furtherance of our highest ambitions.

To be sure, there are serious challenges to be overcome in cyberspace – but a vision of what we affirmatively want cyberspace *to be for* will be critical to get us there.

The Biden-Harris Administration seeks a world where digital connectivity unites the country – and the globe – in an open, interoperable, secure, and reliable internet. Every American should share in the full benefits of that ecosystem, including the economic prosperity it enables, the more responsive, responsible democracy and civic engagement it underpins, and the more vibrant and diverse culture it fuels.

*Every American should share in the full benefits of our digital ecosystem, including the economic prosperity it enables, the more responsive, responsible democracy and civic engagement it underpins, and the more vibrant and diverse culture it fuels.*

In this world, every part of that digital ecosystem, be it a technology, a person, or a system, seamlessly *contributes* to its aggregate stability and security, instead of *detracting* from it. No single component is a source of catastrophic risk, no one Achilles heel is waiting to unleash cascading, systemic failure, and no minor slip-up is capable of producing a massive breach in privacy. Americans who experience vulnerability and insecurity in their daily lives can turn to the internet as a source of support, of comfort, and of power over their own destinies – without the nagging fear of that digital connectivity creating *more* avenues of vulnerability and insecurity. In this world, every digital stakeholder is a source of strength for every other, rather than a source of risk. In this world, all of us are defending each of us.

No system is perfect, however, and neither will be the world envisioned here. But when failure occurs, when malicious actors do manage to breach these systemic defenses, the tools and

procedures to respond, remediate, and recover will be sufficiently accessible, swift, and effective that perpetrators gain little, and what victims there are recover quickly.

Overlapping, aggregated security and resilience will create a world where individual people and organizations no longer need to singlehandedly shoulder the burden of their community's risk. Instead, cyber-safety and security is seamlessly and ubiquitously baked into our everyday lives.

In this world, Americans are free to be enriched, empowered, and enlivened by digital connectivity instead of burdened by it.

## The Challenge

*The unbridled optimism that spoke to so many at the dawn of the internet age has given way to malign actors, big and small, confident in their ability to evade the consequences for the harms they use cyberspace to inflict.*

Computers, defined by the hardware and the software that runs them, are now so complex that it can be difficult to fully appreciate the sum of their constituent parts – a sum which now extends beyond any given physical location. This problem compounds exponentially as computers have been networked together into the vast and increasingly complex digital systems that define our modern lives, economies, and societies. These sprawling arrays of daunting complexity are easy for malign actors to hide in and exploit, and, to date, too challenging for industry or government alone to defend or protect.

As a result, malicious activity in cyberspace has become irresistibly attractive to geopolitical competitors and criminals alike. It enables a level of anonymity, of global reach, and of efficiency of scale that equips countries with asymmetric capabilities that challenge conventional conceptions of defense and deterrence. Criminals and extremists similarly can threaten unprecedented levels of disruption and coercion. Americans' personal information, stolen *en masse* by state-backed actors and online gangs alike, is being weaponized via increasingly sophisticated social engineering or disinformation campaigns. The intellectual property of American universities, researchers, and firms are being stolen and used to circumvent competition or undermine innovation. The unbridled optimism that spoke to so many at the dawn of the internet age has given way to malign actors, big and small, confident in their ability to evade the consequences for the harms they use cyberspace to inflict.

Yet de facto responsibility for managing the risk of this ecosystem has devolved down to the smallest unit of digital actor: individuals, small businesses, and local governments. Critical services for millions can be imperiled because of a single person's failure to recognize a phishing attempt. Federal experts and tech giants alike work to create a safer, more stable digital ecosystem – but implicitly expect everyday Americans to adopt password managers, authentication tokens, and other sophisticated mitigations. Individual cyber hygiene is important and personally laudable, but systemically inadequate; just as individual households working to reduce their carbon footprints cannot alone address climate change, individual users of the internet working to improve their cybersecurity cannot alone realize systemic reform.

★ ★ ★ ★ ★ ★

Technology is supposed to ease our lives, to enable self-betterment, to bring us closer to our loved ones and to our ambitions. But the modern era is also demanding constant digital vigilance of all Americans, many of whom already struggle to make ends meet with the time and technology they currently have. Our internet economy has inadvertently created a digital ecosystem absolutely crucial to today's society, and yet so systemically vulnerable that clicking the wrong link can allow in intruders who encrypt your data and demand a ransom to restore it. Disparate private networks have aggregated into an indispensable public good – but stakeholdership and accountability remain diffuse and opaque. Too many individual Americans are paying the price when this ecosystem fails.

Cybersecurity today too often lacks intentionality. Too many systems are not designed with security in mind, relying on technology end users to keep us safe. It does not have to be this way; if every contributor to our digital ecosystem knew how their part fit into the sum of the whole, and how to contribute responsibly, we could begin building an ecosystem defined by aggregating stability and resilience instead of compounding risk. A world where every component vendor knows how and why it can buy down the risk of its contribution, every network architect knows how to build their systems with resilience as a value, and every Chief Executive Officer knows their Chief Information Security Officer is a profit-protector and not a money-sink, will be a world where citizens are free to share in the benefit of our digital ecosystem.

These are the systemic challenges, in need of transformational solutions, that President Biden and Congress created the Office of the National Cyber Director to overcome.

## The Path

Cybersecurity will forever be a shared responsibility among those who use our digital infrastructure, those who build it, and those who are entrusted with governing it – but it is past time for these responsibilities to be more equitably and proportionally shared by those able to shoulder them. Achieving this vision will require *cooperation* across the many public, private, and international stakeholders in the ecosystem, and it will require *coordination*, so that these efforts are not operating at cross purposes but are instead *mutually reinforcing.* Across sectors and borders, we have both shared infrastructure and shared threat; shared defense is an imperative, not a choice.

> *Individual cyber hygiene is important and personally laudable, but systemically inadequate.*

The Office of the National Cyber Director (ONCD) will help realize this vision and execute the Biden-Harris Administration's cyber agenda through four principal outcomes – outcomes against we ourselves are accountable. First, and above all else, the ONCD will champion **federal coherence** across U.S. government in cyber policy, action, and doctrine. It will **improve public-private collaboration** to tackle cyber challenges across sectoral lines. It will **align resources to aspirations** by ensuring U.S. departments and agencies are resourcing and accounting for the execution of cyber initiatives, assets, and talent entrusted to their care, and considering all possible future such requirements. And it will push forward initiatives across all available avenues in order to **increase present and future resilience**, ensuring our workforce,

technologies, and organizations are fit for purpose today and future-proofed for tomorrow. Ultimately, these efforts mean being purposeful about understanding and overcoming obstacles to cooperation and collaboration, getting the best information into the hands of those who need it, and ensuring all stakeholders – public, private, and international – are able to act on it as fast as possible. We must "crowdsource" our ability to identify and stop transgressors in much the same way they crowdsource their exploitation of us.

Taken together, and in partnership with the National Security Council, the Office of Management and Budget, fellow White House offices, the Cybersecurity and Infrastructure Security Agency and its partner Sector Risk Management Agencies, government stakeholders at every level, and, of course, the private sector, these efforts will improve our ability to collaborate, take Americans off the front lines of cyber conflict, and improve our national and economic security.

ONCD will realize these outcomes through the following lines of effort:

**National Cybersecurity:** ONCD will drive the coordination of missions and programs intended to protect and defend local government and private sector networks, ensuring those programs are equipped with all the information and partnerships (domestic and international) necessary to realize the deepest possible understanding of risk and the greatest possible positive impact.

**Federal Cybersecurity:** The Federal government must both practice what it preaches and serve as an example for other actors to follow, and ONCD will ensure that the world-class cybersecurity we expect of critical private sector actors is reflected and propagated in the departments and agencies with which they collaborate.

**Budget Review and Assessment:** ONCD, in partnership with the Office of Management and Budget, will support departments and agencies as they plan and budget for the future of their cyber resources, including assisting in assessing the performance of relevant programs in achieving their intended effect, and championing those approaches that are models for success.

**Technology and Ecosystem Security:** ONCD will work with government and the private sector to cultivate a more secure digital supply chain, creating an ecosystem of products, devices, and services that are trusted to underpin the very foundations of our digital society.

**Planning and Incident Response:** ONCD will work with Federal agencies charged with preventing and responding to cyber incidents to ensure they are integrated, prepared, and practiced in protecting against, detecting, and responding to malicious cyber activity across government networks and critical infrastructure.

**Workforce Development:** People are the most important part of our digital ecosystem, and ONCD will strive to ensure that both the public and private sectors can benefit from robust and inclusive pathways for cyber talent and that the American people are equipped with the knowledge to secure their own digital lives while contributing to systemic cybersecurity.

**Stakeholder Engagement:** ONCD will work with Congress and the private sector to inform and drive initiatives that depend on the expertise, authorities, and resources of all parties.

## The Urgency

The Biden-Harris administration has prioritized confronting challenges like public health, climate change, economic inequality, and racial injustice not only because of their moral imperative for present and future generations, but also because they are daunting, systemic issues that have compounded for years in difficulty and harm. We must confront issues like these *today* since they will only become more difficult to fix tomorrow, and will be the problems our grandchildren point to when they ask what we did when we had the helm.

*Digital connectivity is already central to our daily lives, but it is also the foundation on which our future lives – lives we cannot yet imagine – are currently being built.*

So too is the task of making cyberspace reflect the values and ambitions we hold for it. Digital connectivity is already central to our daily lives, but it is also the foundation on which our future lives – lives we cannot yet imagine – are currently being built.

Cyberspace, and the technology ecosystem in which it resides, are human creations meant to be crafted to human ends. We look forward to shaping them into a universe defined by its possibilities rather than by its vulnerabilities, a universe known for its promise instead of its failures.