JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

https://oversight.house.gov

Ranking Member Gerald E. Connolly
Opening Statement
Hearing on "Unpacking the White House National Cybersecurity Strategy?"
March 23, 2023

Cybersecurity is a defining political, economic, and national security challenge of our time. From malicious foreign actors' online destabilization and espionage campaigns to ransomware incidents that compromise government and private sector information technology (IT) networks, these attacks have cost the United States billions of dollars and countless critical strategic advantages. In fiscal year (FY) 2021 alone, U.S. federal agencies, which depend on IT systems to carry out operations and protect essential information, were the target of more than 32,500 cybersecurity incidents. In the last half of 2022, cyber attacks targeting governments jumped 95 percent worldwide and cost an average $2.07 million per incident — a 7.25 percent increase from the previous year.

Data breaches also affect the private sector, including educational institutions and health care centers. In 2022, the FBI received almost 801,000 phishing, personal data breach, and other complaints, representing estimated losses of more than $10.2 billion. According to a 2021 survey by research firm AdvisorSmith, 42 percent of small and medium U.S. businesses had experienced a recent data breach. The estimated average cost of data breaches in the U.S. totals almost $9.5 million per breach—higher than any other country—and 60 percent of organizations have raised prices on consumers to cover the costs of data breaches. Experts now predict that the annual cost of cyber crime will climb to $10.5 trillion in the next two years.

Cyberattacks will eventually hit close to home for everyone. For Congress, it was most recently the hack of DC Health Link, which operates a health care system used by many Members of Congress and their staff. Before that, it was the 2015 OPM data breach that exposed the private information of nearly 22 million individuals, including my own personal information. Cyber threats are not new, as information security has been on the Government Accountability Office's (GAO) government-wide high-risk list since 1997.

When it comes to the digital landscape, it is no exaggeration to say that every individual, family, and community is under attack, and everyone is at risk.

For those who are concerned, you are right to be concerned, but we cannot just throw up our hands. We must act quickly and decisively to secure our digital infrastructure, protect the integrity and confidentiality of our data, and preserve public trust in government institutions.

I am proud that the Democrats of this Committee did just that and helped lead the bipartisan fight to establish the Office of the National Cyber Director (ONCD) in the FY 2021 National Defense Authorization Act. The NCD is required to coordinate the whole-of-government effort to elevate Americans' safety in the digital world, including through the development and implementation of the National Cybersecurity Strategy (Strategy). I applaud this Administration's latest initiative to harden our country's cyber defenses. This Strategy is a forward-looking policy framework that bolsters the current constellation of security efforts.

Drawing on bipartisan ideas, including those vested in the recommendations of the Cyberspace Solarium Commission, the Biden-Harris Strategy is a bold, comprehensive plan for government and industry to create a safer digital ecosystem for all Americans. Recognizing that cyber threats cut through all industries and ignore geographic borders, the plan will examine the regulatory landscape to harmonize cybersecurity standards across different sectors and around the globe.

With so much at stake, it's critical that our regulatory landscape allows industry to focus on security outcomes—not duplicative or nonsensical compliance burdens. We also know that if hackers fail to break into one agency or system, they will seek out vulnerable entry points elsewhere. We must, therefore, address the current patchwork of cyber regulations to ensure that cybersecurity protections flow seamlessly and efficiently across industries and government.

The Strategy realigns incentives to ensure the federal government's investments enhance the long-term strength of our cybersecurity posture. For example, it harnesses the federal government's purchasing power to shape market demand for safe and secure technologies.

Through programs such as the Federal Risk and Authorization Management Program (FedRAMP), which my legislation codified last year, we can ensure IT products and services adhere to a standardized approach to so-called "security by design," where security is baked into a product rather than seen as an additional expense or feature.

Additionally, the Strategy redistributes responsibility so that those best positioned to protect the cybersecurity of our citizens, schools, hospitals, and small businesses are required to take reasonable steps to do so. For example, it embraces liability for software companies that fail to use best practices or take reasonable precautions to secure their products.

If we do not hold bad actors—or actors more focused on sales than security—accountable, we disadvantage responsible companies that take the time to follow these best practices, and we increase systematic risk for everyone.

As the Administration works to implement the Strategy, Congress should provide the funding and clarify the authorities needed to ensure its success. As former Chair of the Government Operations Subcommittee and a current member of the Congressional Cybersecurity Caucus, I know it is essential that we invest in modernizing our legacy IT systems and recruit and maintain a federal cyber workforce.

The federal government must also improve its internal practices, reap the benefits of the latest cybersecurity technologies, and increase cooperation with the private sector.

I look forward to understanding how the ONCD will leverage this plan and collaborate with other congressionally empowered IT and cyber-related leaders to promote the kind of accountability our critical federal IT systems need.

###

Contact: Nelly Decker, Communications Director, (202) 226-5181