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
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Hearing on "Enhancing Cybersecurity by Eliminating Inconsistent Regulations"
July 25, 2024

Cyberattacks on government agencies, businesses, critical infrastructure, and private citizens have become alarmingly frequent and sophisticated. The cost of these attacks, both financially and in terms of national security, is staggering. According to data from the Federal Bureau of Investigation and the International Monetary Fund, the average annual cost of cybercrime worldwide is expected to reach more than $23 trillion in 2027. Ransomware attacks against these sectors, for example, increased by more than 50% in 2023. Federal agencies reported more than 32,000 cybersecurity incidents in Fiscal Year 2023. That is an increase of nearly 10% compared to the previous year. In addition, the FBI's Internet Crime Complaint Center received more than 880,000 phishing, personal data breach, and other complaints in 2023.

As I have stated in previous hearings held by this Subcommittee: Data breaches and cyber attacks are no longer novel incidents. That is why securing the systems that are the backbone of the U.S. economy is essential and fundamental to both the public and the private sectors. To this end, the Federal Government has a responsibility to improve cybersecurity outcomes.

To combat cyberthreats, federal agencies conduct comprehensive and multi-layered processes to set and enforce cybersecurity requirements across components of our critical infrastructure such as banks, water treatment plants, and telecommunications infrastructure. For example, the Federal Information Security Management Act and executive orders like Executive Order 14028 on Improving the Nation's Cybersecurity—enacted after the Russian Foreign Intelligence Service perpetrated the SolarWinds' cybersecurity attack—mandate specific cybersecurity practices. Among those requirements are agency-wide cybersecurity programs and risk assessments, incident response protocols, multifactor authentication, and improved event logging.

As National Cyber Director Harry Coker testified in January 2024, there is a clear need for mandatory cybersecurity requirements for critical infrastructure. However, Congress and the administration must not lose sight of our responsibility to improve cybersecurity outcomes. Input from GAO, industry, civil society, and state and local partners indicate that existing regulations vary widely across sectors and at times contain conflicting parameters. This patchwork approach often leaves private, state, and local entities charged with securing critical infrastructure investing less in our collective goal of improving cybersecurity outcomes and more in compliance checking activities, putting our national security and economic stability at risk.

The Biden-Harris Administration has recognized the need to address the overlapping nature of much needed cybersecurity regulations by launching efforts to deconflict and clarify cybersecurity requirements. In March 2023, the National Cyber Director released the National Cyber Security Strategy, which listed "harmonizing regulations to reduce the burden of compliance," as one of its stated policy goals.

In August 2023, the Office of the National Cyber Director—or ONCD—issued a request for information from industry and other partners on the challenges with regulatory overlap and to explore a framework for baseline cybersecurity requirements. All our witnesses here today provided comments and feedback to the ONCD, underscoring the Biden-Harris Administration's collaborative efforts with industry experts to get this right.

In May, The Office of the National Cyber Director also released the first of its kind "Report on the Cybersecurity Posture of the United States". The report assesses the cybersecurity posture of the United States, the effectiveness of national cyber policy and strategy, and the status of the implementation of national cyber policy and strategy by federal departments and agencies.

Among the highlights in the report are actions taken by the federal government during the previous year. Establishing and using cyber requirements to protect critical infrastructure, including through the development and harmonization of regulatory requirements, is the first action listed in the report, which just goes to show how important a priority this has been for the Biden-Harris Administration.

I look forward to hearing today from Dr. Charles Clancy, a senior vice president and Chief Technology Officer at MITRE, about how Congress can support the efforts underway to achieve regulatory harmonization. The goal is to maintain clear and consistent guidance when it comes to cybersecurity requirements. This will improve outcomes by bolstering incident response, enhancing resilience, and reducing costs, ultimately benefitting the American people.

Thank you, I yield back.

###

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