

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-6074  
<http://oversight.house.gov>

**Chairwoman Carolyn B. Maloney**

**Opening Statement:**

***Hearing on U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act  
July 15, 2020***

As our nation reckons with the monumental human and economic toll of the coronavirus crisis, we must look critically at the warnings we had and the decisions made about them.

The most recent Worldwide Threat Assessment of the U.S. Intelligence Community, released in January 2019, warned, and I quote:

“The United States and the world will remain vulnerable to the next flu pandemic or large-scale outbreak of a contagious disease that could lead to massive rates of death and disability, severely affect the world economy, strain international resources, and increase calls on the United States for support.” End quote.

We must ask ourselves what other warnings are going unheeded, and what can we do right now to protect the American people from other catastrophic threats?

Before the unthinkable happens in the future, how can we exercise strategic, decisive foresight to the best of our ability today to ensure we are a nation prepared tomorrow?

That same Worldwide Threat Assessment lists cyberattacks as a top global threat, with China, Russia, Iran, and North Korea waging a silent war capable of shutting down critical infrastructure, breaching sensitive information systems, and jeopardizing critical sectors in America and globally.

The report states, and I quote:

“Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.” End quote.

**Cyberattacks are a critical, complex, prevalent, and growing threat to the nation’s safety and economic security, touching nearly every aspect of our lives.**

This assessment was upheld by recent findings from the U.S. Cyberspace Solarium Commission, which was established by the 2019 National Defense Authorization Act to review the state of our

cybersecurity posture and develop bipartisan solutions for defending America against cyberthreats.

This commission of Congressional, Executive Branch, and private sector cybersecurity leaders sounded the alarm that, in addition to millions of intrusions that disrupt operations in America on a daily basis, we remain vulnerable to catastrophic attacks on critical infrastructure and economic systems that could cause widespread damage and death.

A number of the commission's recommendations fall within the legislative jurisdiction of this Committee.

This includes one that has sparked a high level of interest on both sides of the aisle—the recommendation for a centralized cybersecurity position at the White House to develop and streamline the federal government's strategy, coordination, and response to cyberthreats.

This role was first formalized during the George W. Bush Administration, and then elevated and expanded during the Obama Administration.

But in 2018, then-National Security Adviser John Bolton eliminated the role, reportedly to cut “another layer of bureaucracy.”

The move generated widespread bipartisan concern. In 2019, the United States was rated as the fifth most cyber-secure nation in the world. In 2020, it dropped to the seventeenth.

**Today we will review H.R. 7331, which would implement the Commission's recommendation to establish a National Cyber Director in the Executive Office of the President.**

**This new position would restore that cyber coordination and planning function at the White House.**

In addition, for the first time, it would be backed with resources and statutory authority to lead strategic planning efforts, review cybersecurity budgets, and coordinate national incident response.

A challenge as complex and pervasive as cybersecurity requires that our government be strategic, organized, and ready.

**Democrats and Republicans agree we need a National Cyber Director to ensure we are fully prepared for, and coordinated in, our response to cyberattacks as our nation fights this silent war.**

Our mission today is to gain a detailed understanding of the threats we face, and to thoroughly examine H.R. 7331 as the vehicle for preparing our country against those threats.