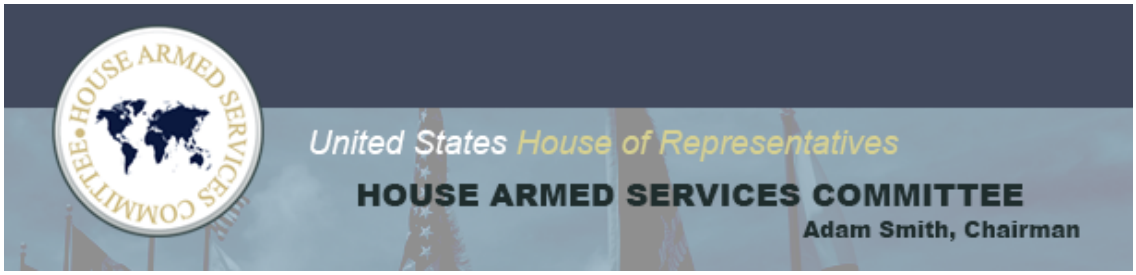
View this email in your browser.




# Opening Statement (As Prepared)
# Chairman Jim Langevin
## Subcommittee on Cyber, Innovative Technologies, and Information Systems Hearing:
## *"Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense"*
## April 5, 2022

*Click here to stream the hearing.*

---

The subcommittee will come to order. Welcome to today's hearing, "Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense."
I'd like to welcome our witnesses:

- **General Paul Nakasone,** the Commander of U.S. Cyber Command and the Director of the National Security Agency,
- and **Dr. John Plumb**, who was recently confirmed as the Assistant Secretary of Defense for Space Policy, and who will serve concurrently as the Principal Cyber Advisor to the Secretary of Defense.

Dr. Plumb appeared in front of the Intelligence & Special Operations Subcommittee on Friday, so this is only his second appearance as a witness for the House Armed Services Committee, and the first on matters related to cyber issues. John, I understand you're a proud Notre Dame alum, I know that Ranking Member Banks is extremely happy to hear this, and I promise not to hold it against you! General Nakasone, it is always great to see you. I have valued our relationship for many years, and I admire your dedication to both your mission and your people. We warmly welcome both of you to today's proceedings and look forward to working together.

As I'm sure you've heard by now, I plan on retiring at the end of the 117th Congress. After nearly 22 years in Congress, I am ready to chart a new course, and have cherished my time serving the people of Rhode Island's Second District, and our women and men in uniform. And over the course of my tenure, I have seen cybersecurity and cyber issues move from the periphery to the center of national security. I hope that I've played some small role in focusing the Congress on these vital matters.

Out of curiosity, I looked back at prior years' National Defense Authorization Acts. In 2001, my first year in Congress, the NDAA didn't even mention the words "cyber" or "internet," not even once. And, there certainly wasn't a combatant command dedicated to cyberspace operations.

Compare that to last year alone, where not only does the word "cyber" appear ***much more***

than once, but last year was the second consecutive year where the NDAA contains an entire chapter, or "title," devoted to cyberspace-related matters. For the Department, Cyber Command has not only been in existence as a Unified Combatant Command for nearly four years, but is conducting operations day-in and day-out in defense of our national security.

In the three years that I have served as Chairman of this Subcommittee, we have had more than 220 separate pieces of legislation, across three NDAAs, enacted into law. This Subcommittee, along with our colleagues from the Senate, have tackled:

- cybersecurity of weapons systems;
- cyberwarfare personnel pay parity;
- cyber targeting;
- support to the private sector and critical infrastructure;
- capabilities to defeat ransomware;
- budgetary authorities;
- cyber requirements for defense contractors;
- and, of the most significance to me, the creation of the National Cyber Director role in the Executive Office of the President.

We no longer have to debate whether we will fight wars in cyberspace, and to some, it may seem crazy that we ever had to have that discussion in the first place. Cyberspace is a recognized domain of warfare, and for better or worse, our service members and civilians are engaged with our adversaries on a daily basis.

Over that same period, the Department of Defense and the military Services have undergone a similar transformation in this space. We have a dedicated Combatant Command for cyberspace operations. We have Soldiers, Sailors, Airmen, Marines, Guardians, and Coast Guardsmen defending our nation in cyberspace. And, we have witnessed the incredible outcomes for our national defense that we can create through cyber means.

And yet, for all the progress that we've made on this front, there can be a sense of déjà vu in the issues we have to address. On workforce matters, for instance, the points we can and should make today are unnervingly similar to what was said in hearings 10, 15, and even 20 years ago. Statements such as "we struggle in competing with the private sector for talent," or "there remains a critical shortfall in our cyber talent." Since 2010, this body has legislated on cyber and STEM workforce issues through 55 provisions, and sometimes, we seem no closer than we were before.

We continue to struggle in elevating considerations for the cyber domain to a level commensurate with how we treat the land, air, sea, and now, space domains. I have been in Congress long enough to know that progress with any important issue is always incremental; however, ***incremental does not have to be synonymous with glacial.***

The responsibility of legislators is tremendous, and we wield the tools at our disposal as carefully as possible. When an issue requires attention, we are judicious in how we direct the Department to respond. Directive actions are powerful, but resorting to these too frequently lessens their effect. That is why we often direct other actions, such as: reports, briefings, quarterly updates, implementation plans, designation of senior officials, and many, many others. We use these to make clear the view of Congress.

We use these tools because they are often successful in accomplishing the desired end state. It is not an exaggeration to say that we have tried to use these alternatives hundreds of times in the cyber context. However, at a certain point, when we are discussing the same issues as our predecessors' predecessors, we have to ask ourselves: "can we continue trying the same types of approaches that don't result in change?"

If we are repeating the same frustrations on an annual basis — about cybersecurity of the Defense Industrial Base, or the readiness of our cyber forces, or the way in which the Department manages cyber issues — then at some point, we must acknowledge a lack of

preparedness to address these critical challenges.

Congress has a great obligation to national security. During my final year in these halls, I am not interested in allowing my successor to inherit the same challenges that plague us today. I look forward to being bold, to pushing for overdue changes, and to working collaboratively with our Members and our witnesses.

With that, I want to again thank our witnesses for appearing before us today. As a reminder, after this open session, we will move to Rayburn 2212 for a closed Member-only session.

I'll now turn to Ranking Member Banks for his remarks.

###

---

**Connect With Us on Social Media:**

**House Armed Services Committee Democrats**
Rayburn House Office Building | Room 2216
Washington, D.C. 20515