....
(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. RES. 575

Expressing the sense of the House of Representatives that all stakeholders in the deployment of 5G communications infrastructure should carefully consider and adhere to the recommendations of ''The Prague Proposals''.

IN THE HOUSE OF REPRESENTATIVES

Mr. FLORES submitted the following resolution; which was referred to the Committee on ______________________________

RESOLUTION

Expressing the sense of the House of Representatives that all stakeholders in the deployment of 5G communications infrastructure should carefully consider and adhere to the recommendations of ''The Prague Proposals''.

Whereas 5G, the next generation (5th generation) in wireless technology, promises the next evolution of communications and information technology services, applications, and capabilities across every sector of business, government, entertainment, and communications;

Whereas the United States, Europe, China, and others are racing toward 5G adoption and upgrading existing networks, which will drive subsequent advances in artificial intelligence, machine learning, smart homes, smart cities, robotics, autonomous vehicles, and quantum computers;

Whereas 5G will make possible the automatization of everyday activities and the use of the full potential of the Internet of Things;

Whereas these developments, while evolutionary, could include risks to important public interests, including privacy, data security, public safety, and national security;

Whereas in a highly connected world, disruption of the integrity, confidentiality, or availability of communications or even the disruption of the communications service itself can seriously hamper everyday life, societal functions, the economy, and national security;

Whereas the security of 5G networks is crucial for national security, economic security, and other United States national interests and global stability;

Whereas operators of communications infrastructure depend on a complex supply chain of technology from a global market of suppliers and service providers;

Whereas government security officials and experts from 32 countries came together in Prague in May of 2019 to work out guidelines for the deployment and security of 5G networks;

Whereas representatives agreed that ‘‘[m]ajor security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions.’’; and

Whereas the Prague 5G Security Conference adopted security recommendations, which have come to be known as ''The Prague Proposals'': Now, therefore, be it

Resolved,

SECTION 1. SENSE OF THE HOUSE OF REPRESENTATIVES.

The House of Representatives—

(1) urges all stakeholders in the deployment of 5G communications infrastructure to carefully consider adherence to the recommendations of ''The Prague Principles'' (as described in section 2) as they procure products and services across their supply chain; and

(2) encourages the President and Federal agencies to promote global trade and security policies that are consistent with ''The Prague Proposals'' and urge our allies to embrace the recommendations of ''The Prague Proposals'' for their public 5G infrastructure.

SEC. 2. PRAGUE PROPOSALS.

The text of ''The Prague Proposals'' is as follows:

(1) ''Policy''.—

(A) ''Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted.''.

(B) ``Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse.''.

(C) ``Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law.''.

(D) ``The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection.''.

(2) ''TECHNOLOGY''.—

(A) ''Stakeholders should regularly conduct vulnerability assessments and risk mitigation within all components and network systems, prior to product release and during system operation, and promote a culture of find/fix/patch to mitigate identified vulnerabilities and rapidly deploy fixes or patches.''.

(B) ''Risk assessments of supplier's products should take into account all relevant factors, including applicable legal environment and other aspects of supplier's ecosystem, as these factors may be relevant to stakeholders' efforts to maintain the highest possible level of cyber security.''.

(C) ''When building up resilience and security, it should be taken into consideration that malicious cyber activities do not always require the exploitation of a technical vulnerability, e.g. in the event of insider attack.''.

(D) ''In order to increase the benefits of global communication, States should adopt policies to enable efficient and secure network data flows.''.

(E) ``Stakeholders should take into consideration technological changes accompanying 5G networks roll out, e.g. use of edge computing and software defined network/network function virtualization, and its impact on overall security of communication channels.''.

(F) ``Customer—whether the government, operator, or manufacturer—must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services.''.

(3) ``ECONOMY''.—

(A) ``A diverse and vibrant communications equipment market and supply chain are essential for security and economic resilience.''.

(B) ``Robust investment in research and development benefits the global economy and technological advancement and is a way to potentially increase diversity of technological solutions with positive effects on security of communication networks.''.

(C) ''Communication networks and network services should be financed openly and transparently using standard best practices in procurement, investment, and contracting.''.

(D) ''State-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles, while taking into account trade obligations.''.

(E) ''Effective oversight on key financial and investment instruments influencing telecommunication network development is critical.''.

(F) ''Communication networks and network service providers should have transparent ownership, partnerships, and corporate governance structures.''.

(4) ''SECURITY, PRIVACY, AND RESILIENCE''.—

(A) ''All stakeholders including industry should work together to promote security and resilience of national critical infrastructure networks, systems, and connected devices.''.

(B) ''Sharing experience and best practices, including assistance, as appropriate, with mitigation, investigation, response, and recovery from network attacks, compromises, or disruptions should be promoted.''.

(C) ''Security and risk assessments of vendors and network technologies should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges.''.

(D) ''Risk management framework in a manner that respects data protection principles to ensure privacy of citizens using network equipment and services should be implemented.''.