

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

SEPTEMBER 24, 2019

Mr. FLORES (for himself and Mr. SOTO) submitted the following resolution; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Foreign Affairs, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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

1 *Resolved,*

2 **SECTION 1. SENSE OF THE HOUSE OF REPRESENTATIVES.**

3 The House of Representatives—

4 (1) urges all stakeholders in the deployment of
5 5G communications infrastructure to carefully con-
6 sider adherence to the recommendations of “The
7 Prague Principles” (as described in section 2) as
8 they procure products and services across their sup-
9 ply chain; and

10 (2) encourages the President and Federal agen-
11 cies to promote global trade and security policies
12 that are consistent with “The Prague Proposals”
13 and urge our allies to embrace the recommendations
14 of “The Prague Proposals” for their public 5G in-
15 frastructure.

16 **SEC. 2. PRAGUE PROPOSALS.**

17 The text of “The Prague Proposals” is as follows:

18 (1) “POLICY”.—

19 (A) “Communication networks and services
20 should be designed with resilience and security
21 in mind. They should be built and maintained
22 using international, open, consensus-based
23 standards and risk-informed cybersecurity best

1 practices. Clear globally interoperable cyber se-
2 curity guidance that would support cyber secu-
3 rity products and services in increasing resil-
4 ience of all stakeholders should be promoted.”.

5 (B) “Every country is free, in accordance
6 with international law, to set its own national
7 security and law enforcement requirements,
8 which should respect privacy and adhere to laws
9 protecting information from improper collection
10 and misuse.”.

11 (C) “Laws and policies governing networks
12 and connectivity services should be guided by
13 the principles of transparency and equitability,
14 taking into account the global economy and
15 interoperable rules, with sufficient oversight
16 and respect for the rule of law.”.

17 (D) “The overall risk of influence on a
18 supplier by a third country should be taken into
19 account, notably in relation to its model of gov-
20 ernance, the absence of cooperation agreements
21 on security, or similar arrangements, such as
22 adequacy decisions, as regards data protection,
23 or whether this country is a party to multilat-
24 eral, international or bilateral agreements on

1 cybersecurity, the fight against cybercrime, or
2 data protection.”.

3 (2) “TECHNOLOGY”.—

4 (A) “Stakeholders should regularly conduct
5 vulnerability assessments and risk mitigation
6 within all components and network systems,
7 prior to product release and during system op-
8 eration, and promote a culture of find/fix/patch
9 to mitigate identified vulnerabilities and rapidly
10 deploy fixes or patches.”.

11 (B) “Risk assessments of supplier’s prod-
12 ucts should take into account all relevant fac-
13 tors, including applicable legal environment and
14 other aspects of supplier’s ecosystem, as these
15 factors may be relevant to stakeholders’ efforts
16 to maintain the highest possible level of cyber
17 security.”.

18 (C) “When building up resilience and secu-
19 rity, it should be taken into consideration that
20 malicious cyber activities do not always require
21 the exploitation of a technical vulnerability, e.g.
22 in the event of insider attack.”.

23 (D) “In order to increase the benefits of
24 global communication, States should adopt poli-

cies 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 solu-

1 tions with positive effects on security of commu-
2 nication networks.”.

3 (C) “Communication networks and net-
4 work services should be financed openly and
5 transparently using standard best practices in
6 procurement, investment, and contracting.”.

7 (D) “State-sponsored incentives, subsidies,
8 or financing of 5G communication networks
9 and service providers should respect principles
10 of fairness, be commercially reasonable, con-
11 ducted openly and transparently, based on open
12 market competitive principles, while taking into
13 account trade obligations.”.

14 (E) “Effective oversight on key financial
15 and investment instruments influencing tele-
16 communication network development is crit-
17 ical.”.

18 (F) “Communication networks and net-
19 work service providers should have transparent
20 ownership, partnerships, and corporate govern-
21 ance structures.”.

22 (4) “SECURITY, PRIVACY, AND RESILIENCE”.—

23 (A) “All stakeholders including industry
24 should work together to promote security and

1 resilience of national critical infrastructure net-
2 works, systems, and connected devices.”.

3 (B) “Sharing experience and best prac-
4 tices, including assistance, as appropriate, with
5 mitigation, investigation, response, and recovery
6 from network attacks, compromises, or disrup-
7 tions should be promoted.”.

8 (C) “Security and risk assessments of ven-
9 dors and network technologies should take into
10 account rule of law, security environment, ven-
11 dor malfeasance, and compliance with open,
12 interoperable, secure standards, and industry
13 best practices to promote a vibrant and robust
14 cyber security supply of products and services
15 to deal with the rising challenges.”.

16 (D) “Risk management framework in a
17 manner that respects data protection principles
18 to ensure privacy of citizens using network
19 equipment and services should be imple-
20 mented.”.

○