COMMENTS BY:
HONEYCOMB SECURE SYSTEMS, INC.

TO:

DEPARTMENT OF DEFENSE
GENERAL SERVICES ADMINISTRATION
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

REGARDING:
FAR CASE 2019-009
FEDERAL ACQUISITION REGULATION;
PROHIBITION ON CONTRACTING WITH ENTITIES USING
CERTAIN TELECOMMUNICATIONS AND VIDEO
SURVEILLANCE SERVICES OR EQUIPMENT

JULY 19, 2019

DEPARTMENT OF THE INTERIOR AUDITORIUM
1849 C STREET, NW
WASHINGTON, DC 20240

PRESENTED BY:
MR. THOMAS R. GOLDBERG
MEMBER, BOARD OF DIRECTORS

Good Morning, and thank you for the opportunity to comment on the implementation of Section 889 of the FY '19 National Defense Authorization Act, banning Huawei Technologies Company, ZTE Corporation (or any subsidiary or affiliate of such entities); and for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

Honeycomb Secure Systems, Inc. is the designer of highly secure ICT equipment, made from state-of-the-art components designed and manufactured at secure sites exclusively within the United States. Some of the sites are approved under the Defense Microelectronics Activity, but most come from special access sites that maintain capabilities and capacity necessary to meet certain national security requirements. These sites serve as the kernels for the reestablishment of US domestic supply chain capacity in the areas the aforementioned Companies now occupy. These sites also serve to provide advanced technologies that exceed the technological capabilities of the aforementioned companies to allow US industry to quickly regain technological superiority in most, if not all, areas where the aforementioned firms now operate.

While this testimony cannot provide details regarding this capability, Honeycomb can describe the nature of the technological advances that are generally available to US firms seeking such access. It is to this point that we direct our comments in response to the questions posed in the Federal Register notice of May 29, 2019:

(1) Beyond the statutory language of the prohibition, what additional information or guidance do you view as necessary to effectively comply with paragraph (a)(1)(B) of section 889?

(1.A) Honeycomb Secure Systems, Inc. requires no additional guidance for its own sake. However, Honeycomb Secure Systems, Inc. recommends that the US Government make available more broadly to affected industries where, and specifically how, they might gain access to capabilities and capacity needed to meet their needs to replace the aforementioned suppliers from whom they obtain components and systems. The US Government has low-volume/high-mix capabilities and capacity to design, fabricate, package, assemble, and test that can serve as the kernels for the reestablishment of US ICT manufacturing in short order. In the case of meeting US Government demand, there is sufficient capacity for such purposes. With modest investment by the US Government (a portion of which is already planned and budgeted), including from industry this capacity can more than meet global demand for secure versions of systems now supplied from abroad. The US Government should do all in its power to ensure that affected industries know of such capabilities and capacity, as well as of the Federal Government's plans and capital resources so that they can be incorporated within their own plans. It should also be noted that this capacity and capability outstrips by nearly a decade most foreign sourced technologies and will provide a competitive edge to any firm that avails themselves of such technology.

(2) *To what extent will compliance with the prohibition in paragraph (a)(1)(B) of section 889 incur additional costs or other burden in providing goods and services to the Federal Government?*

(2.A) This is a complex question that cannot be addressed across the spectrum of products that are currently sourced from abroad. As in the answer to question (1), the US Government already possesses the means to meet most of its needs, it merely needs to shift suppliers to achieve its security needs. The cost for doing so on a one-for-one piece-part basis will, on average, be double the cost currently being paid. Fortunately, the performance enhancement of the new equipment will be far greater than can be achieved by using state-of-the-practice (SOP) equipment, so that the use cost to the US Government will be almost half that which it currently pays. Thus, the US Government will actually save money by requiring this shift to occur.

By way of example, Honeycomb Secure Systems, Inc.'s first generation server has the following attributes that are directly attributable to the components it acquires from the secure supply chain we mentioned above: a) it is 100x faster than any server currently available; b) has 1,000x the storage capacity; and c) consumes 60% of the energy required by any other device of its kind. It is also enjoys a 60% reduction in the cyber-attack surface by virtue of its design that no longer incorporates hard-drives, solid-state or soft-drives. Additionally, because many components incorporate carbon nanotubes the device generates no electromagnetic emissions. Finally, and for the same reason, the device meets all electromagnetic pulse hardening requirements.

On a one-to-one product comparison the Honeycomb Secure Systems, Inc. server has a performance capacity equivalent to ten counterpart servers. Thus, the OEM cost to the US Government for one Honeycomb Secure Systems, Inc. server will be significantly less than any alternative, and the US Government will realize a significant operational cost reduction as well, for a total cost savings approaching fifty percent (50%) of its current costs. Honeycomb Secure Systems, Inc. expects to retain this market advantage for at least five years, based upon our understanding of our competitors' product roadmaps.

Again, one Honeycomb Secure Systems, Inc. server blade is equivalent to ten server blades made by any other firm today. On a blade-to-blade basis, Honeycomb Secure Systems. Inc.'s server saves 40% on energy alone, so on a frame-to-frame basis the US Government will save 400% per frame on energy alone, all the while gaining a tremendous performance enhancement necessary to meet emerging requirements regarding data persistence, AI, and 5G.

(3) *To what extent do you currently have insight into existing systems and their components, sufficient to ensure compliance with paragraph (a)(1)(B) of section 889?*

(3.A) Honeycomb Secure Systems, Inc. has total control over every component design, fabrication, package, assembly and test for anything that enters into any of our products. Honeycomb Secure Systems, Inc. was founded on the principle that in order to achieve security we had to have complete control over our supply-chain. This principle undergirds everything the Company does, and extends to the design of every component, especially every microchip contained therein.

In a more general sense we are benefited by the fact that one of our founders wrote the earliest version of Federal Law establishing supply-chain security requirements for the Department of Defense enacted as part of the 2011 NDAA (Secs. 806, 808). Subsequently this person helped the US Government acquire and site facilities and capabilities from which the Company now draws components and services.

(4) *To what extent do you currently have direct control over existing systems in use (e.g. physical security systems) and their components, as contrasted with contracting for services that are provided by a separate entity (e.g. landlords, contractors)?*

(4.A) Not Applicable. Honeycomb Secure Systems, Inc. currently has no deployed systems in commercial use.

(5) *To the extent that there are gaps in insight or control described in response the previous questions, how much time do you anticipate will be needed to establish insight or control to ensure compliance with paragraph (1)(a)(B) of section 889?*

(5.A) As the answers to the previous questions show, Honeycomb Secure Systems, Inc, will require no time to come into compliance with paragraph (1)(a)(B) of section 889.

(6) *Will the requirement to comply with the prohibition in paragraph (1)(a)(B) impact your willingness to offer goods and services to the Federal government as of the stated effective date? Please be specific in describing the impact (e.g. what types of products or services might no longer be offered, or offered in a modified form, and why).*

(6.A) Honeycomb Secure Systems, Inc.'s willingness to provide secure systems to the Federal government will not be impacted. In fact, the aforesaid prohibition will strengthen Honeycomb Secure Systems, Inc.'s ability to provide products and services to the entirety of the Federal government as more Departments and Agencies become aware of our capabilities, and the provenance of the supply chain that supports our business.