Global Technical Systems Comments on the National Strategy to Secure 5G Implementation Plan

In response to the National Telecommunications and Information Administration (NTIA), United States Department of Commerce request for Comments on the National Strategy to Secure 5G Implementation (Plan Date: May 28, 2020, Docket Number: 200521-0144), Management Services Group, Doing Business As (DBA) Global Technical Systems (DUNS 006543826 | CAGE Code 1MYP5) offers the following comments.

NTIA Questions:

Line of Effort One: Facilitate Domestic 5G Rollout.

1) How can the United States (U.S.) Government best facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, network providers)?

GTS Recommendation: Successful domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem is attainable if the extent of Chinese malign influence is eliminated in US 5G core and edge computing hardware and software, Radio Access Network (RAN) equipment and key enabling technologies specifically, domestic System on Chip (SoC) and micro-server technology supply chains, integration facilities and manufacturing capacity. To accomplish this, a whole of Government and industry initiative comprised of a board of directors from the private and public sectors is recommended, marshaling Commerce, Defense and other agency expertise with leading large and small business expertise across 5G related industries including: equipment manufacturers, chip manufacturers, software developers, cloud providers, end-product system integrators, and network service providers. The objectives of the initiative should be to rapidly establish a secure supply chain for 5G /ICT computing hardware and software. It is recommended this be undertaken in four steps:

1. **Technology threat assessment** – Provide analysis of potential hardware, firmware and software threat vectors that may be enabled by integration of Chinese sourced micro-electronics.
2. **Critical technology identification** – Based on the threat assessment, provide prioritized identification of hardware, firmware and software that represents the greatest potential for exploitation and designate such capabilities for US-only supply sourcing for US 5G network components.
3. **Government investment in US-sourced solutions** – Enable US national industrial capacity to compete globally with China through select investment in Small and Large business manufacturing of identified critical micro-electronics technologies (e.g., microprocessors, micro-servers, Field Programmable Gate Arrays (FPGAs), storage media, including high speed memory, wireless baseband processors, RF baseband and base station equipment and core network hardware).
4. **Enablement of 5G Standards** – Industry and government co-developed telecommunications standards which address the implementation and execution of critical technology and mitigation

of 5G threat assessment. These standards will govern the requirements needed to roll out an effective and secure 5G landscape.

It is important to understand these recommendations are provided with recognition that the Chinese micro-electronics threat goes beyond 5G vulnerabilities into existing and future government, critical infrastructure and vital commercial network ICT architectures. Thus, we provide recommendations for a whole of Government and Industry Initiative. Recognition of the scope of the problem can be found in:

- The SECURE AND TRUSTED COMMUNICATIONS NETWORKS ACT OF 2019 (Public Law 116-124) passed by Congress and signed into law on March 12, 2020
- POTUS issued Executive Orders:
    - EO 13873 "Securing the Information, Communications Technology and Services Supply Chain", 15 May, 2019
    - EO 13920, "Securing the United States Bulk-Power System", May 1, 2020.

The President commits to "facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure here in the United States". Congress and the Administration understand the critical Information, Communications Technology (ICT) industrial base must be stimulated to bring home micro-electronics manufacture and production. But a whole of government and industry response hasn't yet been enabled! Organizations within USD R&E have progressed with their related initiatives, but adequate funding and programmatic approaches have yet to be appropriated at the scale to create a measurable impact. Without this national industrial capacity, the US will continue to be increasingly vulnerable to ICT / 5G adversary threats that place our military, intelligence, advanced technology development and critical infrastructure at risk. By undertaking these recommended steps technology threat assessment, critical technology identification, and investment in US-sourced solutions the United States will have an actionable strategy to overcome the escalating Chinese ICT threat.

2) How can the U.S. Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures?

GTS Recommendation: Swift action is recommended because the challenge is not static. China's share of the global micro-server market has increased dramatically in recent years due to offshoring of integration-level manufacturing activities. To address this escalating National Security emergency, two levels of response are recommended:

1. First, it is recommended that emergency funding be established to foster and promote the research, development, testing, and evaluation of new technologies and architectures, with particular emphasis on micro-electronics computing hardware form factors. While this recommended action will serve to bolster the US position regarding development of future capabilities, by itself, it is insufficient to counter China's global market dominance, insecure ICT supply chain issues and escalating vulnerabilities. Current funding for research, development, testing and evaluation to the DoD is inadequate to address the problem.
   Funding may be allocated from the National Spectrum Auction to a dedicated trust fund to provide for ICT/5G research, development, testing, and evaluation. These activities may be overseen by NTIA through novel, rapid and effective contracting methodologies such as Other

Transaction Authorities and may be augmented by DoD funding to address defense and intel considerations.

2. Second, normal budgetary mechanism(s) should also be put in place to achieve and sustain private sector scaling to provide R&D and industrial capacity for production of critical micro-electronics technologies identified and needed to compete with the Chinese globally. Without direct Government support, US industry cannot achieve manufacturing capacities necessary to compete globally. As the US operates in conjunction with our allies around the world, the security of their ICT architectures is also a significant vulnerability. As a result, our second level recommendation suggests the need for Commerce to work hand-in-hand through an established taskforce with the DoD and industry. Shared responsibility and resourcing are recommended to establish funding to increase industrial capacity in identified critical micro-electronics technology arenas. *Consideration for resourcing innovative Small Business concerns to enable accelerated approaches to manufacturing to scale is necessary to foster emerging advanced micro-electronics such as US made micro-servers.*
   Avenues for funding that should be considered include the National Spectrum Auction described in 1 above, the Defense Production Act, Title III, and Fiscal Year increases to established PE lines in NTIA and the DoD (e.g., OUSD R&E, DMEA, DARPA, Army, PEO C3T, Navy, NAVSEA, NAVAIR...). Using these normal budgetary approaches and mentioned novel funding approaches can serve to rapidly establish needed manufacturing capacities able to overcome 5G and ICT critical technology **threats.**

3) What steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing?

GTS recommendations: The above described approach with a Government and industry taskforce is needed to motivate and incentivize a domestic-based 5G commercial ecosystem to increase 5G research, development, and testing. The objectives or goals for this approach include:

- Determine an approach to identify and fund US R&D and requisite industrial capacity for critical micro-electronics. Addressing R&D through production is necessary including for the following ICT:
    - ICT computing hardware: microprocessors, micro-servers, Field Programmable Gate Arrays (FPGAs), storage media, including high speed memory
    - Communications technologies: wireless baseband processors, RF base station equipment and core network hardware
    - Firmware for fixed and mobile computing hardware and wireless systems
    - Software for fixed, mobile computing systems and core network functions
- Create a micro-electronics industry public private partnership with funding that leverages industry expertise to analyze the affected micro-electronics, determines US-sourcing approaches and provides follow-on budgetary funding to:
    - Enable private sector scaling to meet the challenge
    - Provide critical technology industrial capacity
    - Deliver secure critical infrastructure and government infrastructure for the future
- Establish a path of transition from research, development and testing into integration into the 5G ecosystem.
    - Development of technology roadmap

- Identify key integration partners for research, development, and test transition

GTS has been a leading developer of key technologies in this sphere for the past decade and has made significant investment to combat these escalating ICT threats. *As a small business GTS has led innovations in the micro-server market space with highly secure, US-sourced ICT innovations that can support the broad security concerns of the National Strategy to Secure 5G Implementation Plan.*

4) What areas of research and development should the U.S. Government prioritize to achieve and maintain U.S. leadership in 5G? How can the U.S. Government create an environment that encourages private sector investment in 5G technologies and beyond? If possible, identify specific goals that the U.S. Government should pursue as part of its research, development, and testing strategy.

GTS Recommendation:

1. ***Goal 1 and rationale****: NTIA concentration on micro-electronics R&D, particularly US made micro-server technologies should be a major priority for the 5G strategy*. The SECURE AND TRUSTED COMMUNICATIONS NETWORKS ACT OF 2019 goes a long way in identifying appropriate actions to replace insecure Chinese ICT components. GTS recommends, based on taskforce ICT analysis, that US sourcing for critical ICT components (e.g., micro-servers) be mandated for Government, critical infrastructure, and commercial communications / network architectures. Central to the goal is to establish a US critical 5G/ICT market scale that can sustain industry while it ramps up to address Chinese global competition.

   Goal 2 and rationale*: A Government & industry taskforce must undertake a Technology Threat Assessment.* Leveraging DoD practices for supply chain risk mitigation and best commercial industry practices the taskforce should establish critical 5G/ICT technology vulnerabilities rapidly (in 90 days). Analysis will provide critical data to inform next-step onshoring criteria.

   Goal 3 and rationale*: The taskforce should identify those 5G/ICT technologies most critically at risk of exploitation to establish onshoring or "US-sourcing" criteria. Armed with focused component level data on vulnerabilities, this identification will feed next step policy and funding.*

   Goal 4 and rationale*: The Government should invest in and mandate US-sourced solutions* – Establish the DoD and NTIA emergency and normal budgetary resources to enable US sourced solutions to achieve secure 5G/ICT supply chains.

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure.

1) What factors should the U.S. Government consider in the development of core security principles for 5G infrastructure?

GTS Recommendation: As a National Security Agency (NSA), Commercial Solution for Classified (CSfC), Trusted Integrator (TI) we focus intently on secure architectures based on core security principles. Fundamental to any system security posture are Confidentiality, Integrity and Availability, affectionately known to information security experts as the CIA triad. With the implementation of CIA, a trusted information system can ensure that only authorized users may obtain access, information within the

system is complete and accurate, and information is always available as required. These core principles are directly applicable to the construction of secure 5G infrastructure.

2) What factors should the U.S. Government consider when evaluating the trustworthiness or potential security gaps in U.S. 5G infrastructure, including the 5G infrastructure supply chain? What are the gaps?

GTS Recommendation: As a provider of mission critical computing systems employed in DoD combat systems, GTS has significant experience in the mitigation of supply chain related risk. Maximizing the authenticity and integrity of sub components, firmware and software is critical in the production of secure communication and computing systems. Key factors in the development of core security principles for 5G infrastructures include attributes for the source of supply and functional impact of the component, code or subsystem within the overall security architecture of the system.

1. ***Factor 1 and rationale****: Source of supply, within the supply chain, is of primary concern when evaluating risk associated with core security principles*. Attributes to evaluate of the delivering entity include location, availability, sustainability, integrity, pedigree, ownership, control and influence. Component selection and procurement should include chain of custody and certification of conformance to ordering specifications. Auditable evidence for each of the attributes is required to obtain and use trusted components with a 5G infrastructure.
2. ***Factor 2 and rationale****: Function of, and level of access for, a component, code module or subsystem is an additional concern in the evaluation of risk associated with the trustworthiness of material for use within a 5G environment*. Parts or code (including firmware and microcode) with direct access to key system elements come with significantly higher risk than parts with limited or no direct access to key system elements. For this reason, the consequence of integrating a malicious part can be significant considering the access afforded to the part or code module. Therefore, fundamentals of risk management indicate more attention is required for parts with high exploitation consequence.

3) What constitutes a useful and verifiable security control regime? What role should security requirements play, and what mechanisms can be used to ensure these security requirements are adopted?

GTS Recommendation: A verifiable security control regime is constituted by evidence that controls and procedures are being followed and when not, appropriate corrective action was implemented. Security requirements play a critical role in defining security controls and procedures. Test is the primary method or mechanism to determine if controls are adequate and financial impact (either incentive based or punitive) is the best mechanism to ensure the security requirements are adopted. The recent push within DoD to adopt CMMC is a good example, in which contractors that do not meet the security controls can no longer submit an acceptable proposal. In this case, failure to meet the security requirements is heavily punitive for the noncompliant entity.

4) Are there stakeholder-driven approaches that the U.S. Government should consider to promote adoption of policies, requirements, guidelines, and procurement strategies necessary to establish secure, effective, and reliable 5G infrastructure?

GTS Recommendation: Stakeholders, including government, critical infrastructure, and public-private authorities (e.g., DoD, other Agency and State/local government networks, utilities, and quasi-public / private networks) all have different user objectives for their networks but the same or similar need for trusted network compliance. Providing a Federal "Secure Network Policy which include mandates and guidelines for component architecture (dependent on the criticality of the component and susceptibility to exploitation) would provide a common starting point for stakeholders. Implementing appropriate inspection and test protocols also based on criticality and potential for exploitation should be included in those policy requirements. Federal and State agencies should commit cyber resources to support stakeholder network design, and define and publish approved secure component lists. These lists should differentiate security requirements appropriate for level of criticality of network function and enable economically driven choice in component architectures appropriate for the security standard they operate under. It is critical to implement such provisions in a manner that supports the competitiveness of supply chain members, including sub component and foundry level production.

5) Is there a need for incentives to address security gaps in 5G infrastructure? If so, what types of incentives should the U.S. Government consider in addressing these gaps? Are there incentive models that have proven successful that could be applied to 5G infrastructure security?

GTS Recommendation: Financial incentives are the most effective form of enticement for commercial entities. Performance based incentives have proven effective in defense and commercial industries. Tax and insurance related incentives are additional forms of indirect incentivization that are available to influence positive security outcomes. The government may also dictate which entities may use 5G spectrum and therefore may limit access to those frequencies to only providers that meet certain security standards. Disbarment, disqualification and financial penalties are an additional form of incentive with less effectivity since some organizations will decide not to participate due to risk of financial or business stature loss. Positive incentive models encourage wider participation than punitive incentive models. We believe a combination of the two can be effectively applied to 5G infrastructure security.

Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

1) What opportunities does the deployment of 5G networks worldwide create for U.S. companies?

GTS Recommendation: 5G networks worldwide create an opportunity for US allied countries to implement a secure connection space for companies who adhere to USG requirements. These companies will be allowed and incentivized to deploy technical solutions to allied countries who have similar concerns to eliminate Chinese influence. We discuss the global elements of the Chinese threat in 3 ways: 1) Importance of understanding that the micro-server form factor market is accelerating in diverse applications; 2) Escalating dominance of Chinese in micro-server market has grown 50% in last 5 years and surpassed $20B sales (micro-server alone) globally; 3) Huawei has demonstrated their market dominance can sway even allied approaches to instantiation of 5G architectures and that those market decisions have implications for US/allied network security. Until US micro-electronics companies can compete on an equal footing, Chinese expansion will continue.

2) How can the U.S. Government best address the economic and national security risks presented by the use of 5G worldwide?

GTS Recommendation: The previously detailed 3 step solution is recommended. Until US micro-electronics companies can compete on an equal footing, Chinese expansion will continue.

3) How should the U.S. Government best promote 5G vendor diversity and foster market competition?

GTS Recommendation: Require US / allied sourcing/trusted supply chain practices for 5G architecture development in the US and influence allies to support same.

4) What incentives and other policy options may best close or narrow any security gaps and ensure the economic viability of the United States domestic industrial base, including research and development in critical technologies and workforce development in 5G and beyond?

GTS Recommendation: Require US / allied sourcing/trusted supply chain practices for 5G architecture development in the US and influence allies to support same. Follow 3 steps to identify critical technologies to onshore.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

1) How can the U.S. Government best lead the responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market?

GTS Recommendation:

1. Recognize there are malign and insecure supply chain actors
2. Develop alignment of international standards bodies (IEEE…) around secure supply chain processes including inspection methodologies

2) How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?

GTS Recommendation: It is critical that one of the charters of the task force be to speak on behalf of the U.S. Private sector. This is done within the semiconductor market via SIA. Since SIA is made up of multiple industry leaders it has the ability to speak on behalf of a majority of the semiconductor community. This allows for the best representation of the needs within semiconductors. The 5G taskforce should adopt these lessons learned and implement them.

3) What tools or approaches could be used to mitigate risk from other countries' 5G infrastructure? How should the U.S. Government measure success in this activity?

GTS Recommendation: Employ risk mitigation and quantification models consistent with aforementioned core and supply chain security fundamentals.

4) Are there market or other incentives the U.S. Government should promote or foster to encourage international cooperation around secure and trusted 5G infrastructure deployment?

GTS Recommendation: Per previous discussion, fund industrial expansion of US micro-server and other critical 5G technologies.

5) Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications infrastructure supply chain. Are there other models that identify and manage risks that might be valuable to consider?

GTS Recommendation: NIST 800-161 for supply chain security and the process by which the NSA evaluates technologies under the Commercial Solutions for Classified (CSFC) Trusted Components List utilizing NIAP protection profiles, commercial and national test labs and rigorous test methodologies.