Tenet3 has studied 5G cyber-physical, logical, economical, and political systems with an eye towards understanding how the US government can assess risk and develop security principles that will guide the roll out of 5G infrastructure. The company has also performed qualitative and quantitative analysis of 5G standard setting organizations including 3GPP. Tenet3's study and 3GPP analysis insights inform the responses below.

In response to Line of Effort 2: Assessing Risks and Identifying Core Security Principles for 5G Infrastructure

Tenet3 recommends the adoption of risk assessment and security principles inspired from publications of the Department of Defense's previous work under the Anti-Tamper and Software Protection Initiative (ATSPI). The principles are rooted in an Electronic Warfare Threat Model where system *vulnerabilities* are assessed based on the enumeration of (i) critical system components and their susceptibilities; (ii) access points, resulting attack paths, and accessible data and functions needed to expose these susceptibilities, and (iii) technical capabilities enabled by the operating environment to leverage (i) and (ii) for an exploit. This model thus asserts that *a system and its operating environment defines its own threats*. The system owns an inherent set of susceptibilities (weaknesses) and access points; and thereby permits associated exploits when the operating environment enables it (which can be extended to include the system's lifecycle and supply chain). This system centric approach to risk assessment requires only system knowledge (not threat intelligence) to set an upper bound on vulnerabilities. The actual number of encountered vulnerabilities will be a subset of this upper bound. This approach to risk assessment can be mechanized and scales well with system complexity.

Q1: Factors the U.S. Government should consider in developing core security principles for 5G infrastructure

Three core security principles, hereafter defined as the *3 Tenets*, comprise secure design methodologies and assessment tools under the above threat model. The tenets require (Tenet 1) system designers identify and focus their security efforts on mission critical components; (Tenet 2) access to critical system information, data, and functions be moved 'out of band' to an attacker; and (Tenet 3) dynamic sensing and response technologies are deployed to mitigate a threat's capabilities automatically. Tenet 1 minimizes the number of potential susceptibilities within the system to consider. Tenet 2 minimizes attack availability by limiting points of access to the attacker. Tenet 3 minimizes the chance of an adversary having the resources and capabilities to successfully complete an attack under system operating timelines and conditions. For example, nonstationary system patterns with hard detection penalties increase the knowledge needed to attack and discourages potential adversaries from initiating an attack. Multiple analyses performed at the Air Force Research Labs and Tenet3 have shown how system security models carried out under the above threat model and security principles (*3 Tenets*) yield *strategic* recommendations to improve system security based on quantitative risk and security measurements.

This threat model and security principles are suitable to assess 5G infrastructure for the following reasons:

1. **The global and high profile 5G cyberspace requires *systems-centric*, strategic risk and security assessment.** The high-profile impacts of 5G in global commercial sectors and international governments means Murphy's Law applies: if anything can go wrong, it will, or: given a vulnerability, no matter how small or modestly impactful, there will be an adversary motivated and skilled enough to exploit it. It is impossible to enumerate all adversary actions. Assessments thus based on hypothetical attacker means, motives, and opportunities will have blind spots. This is especially true for a complex global technology like 5G. Strategic and systems-centric risk and security assessment approaches pioneered by the DoD ATSPI defines threats by what the system *is*, rather than by what an attacker *could be*.

2. **The threat model is successfully practiced for quantitative risk and security assessment.** Quantitative risk and security assessment follow directly from the three security tenets. Tenet3 has produced *data-*

driven risk and security metrics based on a knowledge-enabled system model. The model emphasizes *what* a system is composed of and *how* system components are integrated by the mathematical abstraction of a graph. Nodes define components, arcs define relationships, and properties of any type (property values, datasets, other models) are attached to nodes and arcs as a list of attributes. This paradigm allows statistical, computer science, and machine learning algorithms to process information about a system, the data it produces, and its physical and logical structure to build quantitative risk and security metrics. The model further captures information to automatically identify a system's susceptibilities, the corresponding information and components of a system needed to exploit a susceptibility, and to assess the capabilities needed to perform an attack. Tenet3 has shown, for example, how to integrate per-component risk assessment measures into a total system risk assessment score in a statistically sound manner. The company has also defined theoretical 'games on graphs' to identify an optimal allocation of sensing, response, and other mitigation tools to system components that maximizes the capability an attacker needs to successfully execute an attack on a system.

3. **The threat model and security tenets are generic. They are applicable to economic and political assessments as well as those of cyber-physical and logical systems.** The security of 5G infrastructure is not simply a problem of certifying that 5G infrastructure components are "secure". National 5G security can be compromised in fundamental ways through economic and political means. Unless incentivized otherwise, buyers in commercial technology marketplaces tend to purchase based on price, all else being equal, particularly if they have (false) confidence that a technology's security controls yield an acceptable level of security. Furthermore, buyers seldom act altruistically. It is likely that a cheaper 5G device will be preferred over one appearing to offer an equal amount of user security, but may include features (trojan payloads, backdoor network access, snooping protocols, etc.) that place the National 5G infrastructure at risk. Geopolitics further drive 5G security at both the national policy and 5G standard setting levels. National polices, including those the Department of Commerce has developed to mitigate the use of Huawei technology in the United States, have altered global cellular and microelectronics ecosystems in ways that will directly bolster the security of National 5G infrastructure. At the same time, those polices may introduce unforeseen security vulnerabilities caused by ecosystem disruptions and other supply chain factors. Polices that compromise security may also be embedded in the 5G standards devices are required to adopt.

4. **A knowledge-enabled modeling paradigm can capture the economic and political systems driving 5G**. From expert knowledge and data captured in government and business reports, a complex web of sector or national dependencies among the 5G and microelectronic industries or geopolitical relations can be captured with rich metadata. The models can be subsequently used to identify sectors or nations that are ripe for exploitation. These nations and sectors may introduce susceptibilities that are easy for adversaries to access and represent the simplest path to severely disrupt a system. The model can further be evaluated for "what-if" assessments of changes to economic and foreign relations landscapes. The same quantitative risk assessments performed over models of physical systems can inform policy analysts about what would otherwise be hidden risks and impacts of a policy implementation. Data from voting records, meeting minutes, and other documents publicly published from the meetings of 5G standard setting organizations can be used to develop system models of organizational relationships and alliances among member organizations. The same data can be used to annotate the model with information about organizations' past voting trends, technical and policy interests, previous alliances, and data about their past 3GPP participations.

Q2: Factors to consider when evaluating trust or potential security gaps in US 5G infrastructure and supply chain

It is essential that the United States participate, or at a minimum carefully observe the 5G standards setting process carried out in 3GPP SSO meetings. These international standards establish the required functionality, protocols, system components and technologies necessary for a device to be declared "5G compliant" and be usable in global 5G systems. Standards that intentionally or otherwise induce a security risk to U.S. 5G Infrastructure introduce fundamental susceptibilities and infrastructure access points that are difficult or even impossible to defend. For example, the government may be powerless to prevent companies from implementing specific aspects of 5G standards strictly for devices used in the U.S. Such devices would become locked out of the global 5G ecosystem (and potentially some U.S. 5G subsystems) and eventually cause a partitioning of 5G, and by consequence the Internet at large, between the U.S. and the rest of the world. The standards proposed, discussed, amended and passed are mainly driven by complex politics that play out among 3GPP member organizations – security considerations are not a primary concern. Organizations who are sponsored by other nation-state interests barter in ways to encourage an organization's (and by extension their nation's) preferred standards to be passed. U.S. interests are scarcely and ineffectively represented in these political standard setting games.

Moreover, **the United States should not blindly "accept" that 5G standards establish any base level of security or risk mitigation.** Standard proposals developed under affiliate working groups are done strategically. Proposals from these small member working groups are presented to the 3GPP body at-large during meetings. Such proposals may be considered "vetted" and "recommended" by an affiliate working group and could come under less technical and security scrutiny when presented to the 3GPP SSO for approval.

In response to Line of Effort 4: Promoting Responsible Global Development and Deployment of 5G

Q1: How the U.S. Government can lead responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market.

Tenet3 offers three responses to this question:

1. **Monitor the international development of 5G technology standards by a data-driven approach.** Such monitoring can yield insights including voting trends and block voting tendencies among member organizations. Detailed monitoring also provides a quantitative understanding of topics of interest by particular organizations and the larger standards setting bodies like 3GPP. Monitoring also allows real-time tracking of trends that capture the degree of nation influence in 3GPP meetings.

2. **Create programs supporting U.S. subject matter experts to observe and participate in 3GPP SSO events.** Due to the complex dynamics in the 3GPP environment, a team that monitors 3GPP activities for the interests of the government may be more effective if staffed with experienced personnel, such as former employees of U.S. and allied telecommunication companies who have previously participated in the standards setting process.

3. **Introduce market incentives to purchase equipment from vetted suppliers.** An incentive structure is especially necessary as 5G technologies roll out to ever more rural areas of the country. Rural Internet and cellular service providers are pressured to deploy infrastructure as efficiently and economically as possible. This is because rural areas are not dense (reducing subscriber revenue) and requires the planning and deployment of new infrastructure in remote areas. Lacking incentives to invest in new technology with an emphasis on security over price, rural 5G infrastructure will become particularly vulnerable to susceptibilities and unexpected system access points. This suggestion must also be considered in light of the fact that 5G will create new technology markets. 5G equipment will not be exclusively purchased by cellular and internet

service providers. The broad adoption of 5G will pressure small businesses and start-ups to modernize their existing products with 5G chips to enable capability relevant in the interconnected future 5G will usher. New technology start-ups may even rise to create unique infrastructure devices that facilitate 5G's dense infrastructure requirement (the millimeter-wave portion of the 5G spectrum will likely be clutter limited in range compared to 3G and 4G). Without incentive for this market to purchase chips and technology from vetted and preferred suppliers, small businesses will be economically pressured to purchase the cheapest technology that simply works without considering national security ramifications.