Gigamon Comments to Inform the Development of an Implementation Plan for the National Strategy to Secure 5G RIN #0660-XC04, Docket No. 200521-0144

Gigamon appreciates the opportunity to respond to NTIA's request for comment on developing an Implementation Plan for the National Strategy to Secure 5G. As described in greater detail below, Gigamon recommends that:

(1) network traffic visibility be considered a core security principle for 5G infrastructure; and
(2) the U.S. Government encourage broad industry participation in the 5G standards development process by offering incentives to help defray the associated costs.

Gigamon delivers network visibility and analytics for digital applications and services across physical, virtual and cloud infrastructure, enabling organizations to run fast, stay secure, and innovate. Since 2004, Gigamon has been awarded over 75 technology patents, and provides products and services to 80 percent of the Fortune 100 and the majority of the world's Top 10 banks, healthcare providers, technology companies, mobile operators and government agencies. Most significantly for the purposes of this response, Gigamon is the market leader in the service provider vertical. Gigamon's comments reflect the lessons learned servicing its customers.

Line of Effort 2: 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?*

Gigamon recommends that the U.S. Government consider visibility of network traffic (e.g., the ability to see and secure traffic that moves along a 5G network) as a core security principle for 5G infrastructure and should be incorporated as early as possible in the design and build stages. Any 5G network which has areas which cannot be monitored by threat detection instrumentation creates a blind spot which threat actors can and almost certainly will exploit. As such, core security design should include visibility of all network traffic. The technologies to do this already exist and are widely deployed.

Notably, network traffic visibility does not require analysis of traffic content, which is often difficult because network traffic is increasingly encrypted, traffic volumes far exceed the ability to economically scan the contents, and law and policy may restrict content analysis. Traditional traffic analysis (volumes, times, cadence), network metadata analysis, and other analytic tools are able to effectively and rapidly detect abnormalities which may indicate potential risk. Armed with such data, network defenders and threat hunters are more likely to detect threats and mitigate risk.

5G service providers simply cannot exclusively trust host-based reports as the host may be compromised. In fact, the risk of compromise is elevated for virtual network infrastructure as the compromise might not only exist in the virtualized application, but in the hypervisor underneath it, or by a hardware or software implant. However, network packets flowing over monitored links cannot be concealed. Even if traffic is encrypted or masqueraded as non-malicious traffic (stenography), the unexpected additional flows can be detected by sufficiently capable analytic approaches provided there is adequate visibility throughout the network. While visibility is something which can be retrofitted post-deployment, it will be less expensive, far less intrusive, and more effective if it is baked-in early in the life cycle.

Line of Effort 4: Promote Responsible Global Development and Deployment of 5G

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

Gigamon recommends that the U.S. Government encourage broad participation from the private sector in the development of 5G standards by offering incentives to defray the costs (including opportunity costs) of engagement. This would enable resource-limited organizations that are (or will be) impacted by emerging standards to participate and also help counter the efforts of other nations to stack and influence standards groups. In addition, enabling participation by companies that have not historically engaged in the process will bring new and diverse technical concepts and approaches to the table.

Gigamon believes that incentives will encourage earlier and more robust participation from organizations other than service providers and 5G equipment manufacturers who may have specific industry needs which should be addressed by emerging 5G standards. For example, the banking industry currently uses 3GPP network connections for a majority of consumer transactions, which makes authenticating customers using mobile identity challenging for both themselves and the service providers. In addition, automobile manufacturers are increasingly developing equipment that is highly dependent on mobile connectivity. Ensuring adequate information assurance over these channels will be critical as lives will be at stake. These are just two examples of industries that should engage but there are many more.

As a real example of the challenges created when interested and impacted parties are not at the table, Gigamon offers the TLS 1.3 example. The US banking industry uses TLS extensively but their involvement in the ten-year long development of TLS 1.3 occurred only towards the end, when they realized that certain aspects of the protocol would cause significant problems for their security and management infrastructure. The IETF had been largely pursuing a usage model which had an external user, and web-based infrastructure, with the traffic transiting the Internet. The use of TLS inside infrastructures and datacenters had not been considered. The last-minute engagement by the banking sector and other impacted parties did not, however, change the design of the protocol. In fact, at the vote at IETF101, the late engagement of the banks and associated vendors (including Gigamon) was seriously criticized. As such, the standard went ahead, and many organizations are struggling to handle the changes it introduced.

To avoid such outcomes in the future, Gigamon recommends the introduction of incentives which facilitate small and medium sized organizations with direct involvement in the 5G space and organizations from allied market verticals to participate in standards developments so that their needs can be addressed, or alternatively, issues identified early enough for alternative approaches to be considered.