Leadership and Security Strategy to Enhance the National 5G Implementation Plan

Federal Data Systems LLC[1] and Information and Infrastructures Technologies, Inc.[2] welcomes the opportunity to provide this joint response to the National Telecommunications and Information Administration's (NTIA) request for public comments to inform the development of an Implementation Plan for the National Strategy to Secure 5G [Strategy].[3] We believe that a keystone component of any subsequent implementation plan is a comprehensive security evaluation and assessment program. Each strategic line of effort hinges on the United States' (US) capability to lead, develop, and implement a High-Assurance Security Evaluation and Trusted Delivery Program for 5G infrastructure.

High-Assurance Security Evaluation and Trusted Delivery Program

A High-Assurance Independent Evaluation and Trusted Delivery program is a rigorous evidence-based risk assessment model to identify and mitigate risk in every key element of the source, supply chain, implementation, and maintenance ecosystem and lifecycle. Aspects of Trusted Delivery models have been employed by US Tier 1 and Tier 2 carriers, and carriers in Canada and the UK over the past eight years, have matured for a number of major telecommunication vendor technology solutions, including 3G/CDMA, LTE (TDD, FDD) and preliminary 5G implementations[4]. Further expansion of the approach has been hindered by the lack of formal regulatory support and guidance. Trusted Delivery programs are proven to address US Government telecommunications security concerns and to directly mitigate threats and reduce security risks, and have been supported by CFIUS as a key element in mitigating explicit national security threats and risks.

---

[1] Federal Data Systems LLC (feddata.com) is a leading provider of information technology products and services to government and commercial markets. Founded in 2006, FedData specializes in the design, delivery, implementation and monitoring of automated systems with a corporate emphasis on infrastructure design, data security, incident response, continuity of operations, and information assurance. Through several prime contracts with the United States Intelligence Community, FedData provides design and implementation of sophisticated IT networks for systems of national importance.

[2] Information and Infrastructures Technologies, Inc. (iit-corp.com) IIT provides the private and public sectors with vendor-neutral solutions that are advanced, comprehensive and complete. Reducing business and security risks our clients face today and may face in years ahead is critical to safeguarding and securing business and government infrastructures and environments.

[3] National Strategy to Secure 5G of the United States of America, March 2020, available at https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

[4] A recommendation for a Trusted Delivery model was included in comments to FCC Docket 18-89, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Notice of Proposed Rulemaking on 7/2/2018, https://ecfsapi.fcc.gov/file/10702176805071/2018%200702%20(2)%20National%20Security%20Reply%20Comments%20-%20FINAL.pdf.

Trusted Delivery Credibly Addresses Supply Chain Security Lifecycle Vulnerabilities

Trusted Delivery programs reduce supply chain risk through evidence-based comprehensive measures that reliably address real world threats. A Trusted Delivery program also addresses a critical element of the National 5G Strategy by helping to promote a more secure and reliable 5G infrastructure. Such a model provides the end user assurances that systems (hardware, software, and firmware) precisely match those which were fully evaluated by an independent laboratory. Enabled by initial comprehensive evaluation, Trusted Delivery methodology extends security assurances across the full lifecycle of the technology deployment—baselining, addressing patches, new releases, and upgrades. This methodology identifies and mitigates vulnerabilities, weaknesses, and exposures not detected through conventional Certification and Accreditation (C&A) or Security Evaluation, and continuously applies initial and follow-on lifecycle testing mapped to analyzed threats and vulnerabilities, thus enabling continuous evaluation of vulnerabilities to evolving and newly discovered threats; dramatically improving quality of software and source code, which greatly improves performance. This approach forces a high level of maturity and diligence in vendor development practices, and continually saves money and resources in delivering essential cybersecurity protection. The policies, standards, and processes in a Trusted Delivery program provide assurances against undocumented changes being made by a vendor or third party who touches the supply chain or existing infrastructure. Additionally, increasing concerns about our nation's dependence on the foreign supply of critical information and communications technology can be met by these effective assurances and mitigations.

Trusted Delivery Program Exceeds US 5G Implementation Strategic Goals

A High Assurance Security Evaluation and Trusted Delivery Model applies to each strategic leadership and security goal set out by the US 5G Implementation Plan: *(1) Facilitating domestic 5G Rollout; (2) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (3) addressing risks to the US economic and national security during development and deployment of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of secure reliable 5G infrastructure.*

Line of Effort One: Facilitate Domestic 5G Rollout

(1) *How can the US 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)?*

In addition to the private sector economic benefits of enabling true domestically developed 5G and related technologies, there is a crucial need to resolve the key underlying issue that forced this national conversation: deliver a secure 5G solution which directly addresses threat concerns, makes the US less dependent on foreign-based critical supply chains, and establishes a supply chain security solution that more completely addresses the inherent supply chain security challenges and unease which exist today. Trusted Delivery methodology credibly addresses critical supply chain

security vulnerabilities on a continuous basis and promotes a sustainable methodology to comprehensively and proactively address actual analyzed threat concerns. It bears repeating that implementing a Trusted Delivery model places an independently-governed validation process between the developer and the end user, ensuring that software binaries match independently compiled binaries which were built using only fully evaluated source code and; that they do not contain unauthorized changes and; that approved hardware designs were fully adhered to while insulating the process from dangerous supply chain interdictions.

(2) *How can the US Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures?*

The US Government has a unique opportunity to simultaneously foster technical innovation and enhanced security across the evolving 5G ecosystem as e=well as encourage, and where possible, require a "Defense-In-Depth" approach be applied to new technologies and architectures. Implementation of High Assurance Evaluation and Trusted Delivery methodologies would significantly improve and enrich the 5G Strategy because such a model simplifies prioritization of efforts and provides very precise insights into potential weaknesses which require unique attention in network security monitoring, incident response preparedness, and a highly effective process for testing and continuously improving the Defense-in-Depth process. The High Assurance process allows for the proactive elimination of generally undetectable vulnerabilities and exposures and precise rapid adjustments to protocols, based on a continuous cyber threat analysis process and detailed testing to confirm potential exposures.

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

The most effective approach to date applied by commercial carriers attempting to elevate and harden telecommunications security standards has been to require the implementation of methods such as independent High Assurance Evaluation and Trusted Delivery as a condition of competing in the market place. There are several readily available cost models that facilitate this approach. Coupled with a "buy US" strategic communications campaign, such an approach would cause capable US contributors to the 5G technology development effort to be more favorably considered.

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

One continuing area of R&D shortfall is the need to continue "on-shoring" of improved microelectronics device foundry capabilities and capacity, and the development of high-impact

security strategies. While there are many focus areas worthy of R&D consideration, some priority is needed on developing counterfeit mitigation solutions, including comprehensive validation and verification protocols that can be reliably implemented and that are fully repeatable processes to eliminate a large family of dangerous threats. A process is needed to support such an effort that would provide continuous threat analysis inputs to drive these complex development challenges.

Line of Effort Two: Assess Risk 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?

Implementing an evidence-based approach to verify the provenance of people, processes and technologies used in 5G should be a core security principle. Independent assessments remain a key tool. Implementation of High Assurance Evaluation and Trusted Delivery methodologies would significantly improve and enrich the 5G Strategy. It simplifies prioritization of efforts and provides very precise insights into potential weaknesses that require unique attention in network security monitoring, incident response preparedness, and a highly effective process for testing and continuously improving the Defense-in-Depth process. The High Assurance Process allows for the proactive elimination of generally undetectable vulnerabilities and exposures and precise rapid adjustments to protocols, based on a continuous cyber threat analysis process and detailed testing to confirm potential exposures.

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

Implementation of the verifiable Independent High Assurance Evaluation and Trusted Delivery process directly addresses this concern and seriously reduces the gaps that currently exist in direct threat mitigation or elimination. Any unverifiable claims or limited transparency into the people, processes and technologies used to realize 5G capabilities and services should be cause for concern.

(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?

The implementation of High Assurance Evaluation and Trusted Delivery methodologies would significantly improve and enrich the 5G Strategy. By delivering protocols that fully evaluate and validate mandates security processes this approach offers a solid best practice level method to consistently address these issues on a continuous basis. This approach simplifies prioritization of efforts and provides very precise insights into potential weaknesses that require unique attention

in network security monitoring, incident response preparedness, and a highly effective process for testing and continuously improving the Defense-in-Depth process. The High Assurance Process allows for the proactive elimination of generally undetectable vulnerabilities and exposures and precise rapid adjustments to protocols, based on a continuous cyber threat analysis process and detailed testing to confirm potential exposures.

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

Integration of desired security outcomes, including explicit verification solutions into procurement requirements would help establish the desired outcome in this regard. There is also a need to help reduce the cost impact of forcing commercial entities to deliver next generation security capabilities in their network infrastructures. One approach that has been repeatedly applied in industry of the past several years is to allow the vendors to address the costs of security relevant measures, in High Assurance and Trusted Delivery through providing "invoice credits" to the end user. This approach has zero cost impact for end users and significantly reduces the actual costs for the selected vendors.

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

One industry proven approach for incentivizing improvements is by certification of adherence to a mandatory Maturity Model. This approach would promote a level competitive playing field, evolve, and adapt to changing threats and enforce requirements that are critical to eventual desired security outcomes.

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

(1) *What opportunities does the deployment of 5G networks worldwide create for US companies?*

The primary opportunities for US companies in the 5G market spaces are access to global markets, as well as future participation in Tier 1 and Tier 2 US carrier markets, which are currently fully dominated by essentially foreign-based international telecom vendors. Participation will also present risks from adversaries that may not have existed or were minimal in the US domestic market.

(2) *How can the US Government best address the economic and national security risks presented by the use of 5G worldwide?*

The US Government should develop, apply, and adapt different strategies to account for the US ability to influence or shape particular markets. When possible, encourage and incentivize allies to adopt similar security frameworks and sharing of threat information. Apply Zero Trust model, including deep evaluation and trusted deliver solutions and assume the adversaries have unfettered access to those networks. An assumption of available and exploitable vulnerabilities promotes the creation of more granular, Advanced Persistent Threat – based network monitoring solutions and more effective and timely incident response protocols.

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

Vendor diversity and increased competition would be incentivized by the US Government through the encouragement and adherence to open standards whenever practicable. Currently, virtually all major international telecom vendors participating in this market leverage highly proprietary technology solutions, creating complex barriers to market penetration by emerging vendors; an overwhelming obstacle to market entry for emerging US vendors.

(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*?

Enforcing threat-based security standards in the US 5G market would go a long way toward satisfying this goal. Also, by applying a verifiable independent High Assurance Evaluation and Trusted Delivery process across the domestic industrial base the US would be instilling a solid security foundation that would provide benefits beyond the 5G industry.

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

(1) How can the US 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?

By requiring the application of High Assurance Security Evaluation and Trusted Delivery methodology to all vendors and networks the US Government further enhances the US position in the 5G marketplace and reduces the risk presented to US Government users of commercial 5G services. This, in turn, elevates infrastructure security and enables a threat-based security solution which can continuously evolve throughout the deployment lifecycle as the threat landscape changes.

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

Supporting the application of open standards wherever possible makes it possible for US private sector participation by lessening the impact of what are now largely proprietary solutions in the market. This creates a level playing field for new technology developers to credibly enter the market. Minimizing the market friction caused by proprietary standards will encourage innovation and reduce the time to market for new features and services.

(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?*

To effectively mitigate risk from the 5G networks of other countries calls for the creation of a security framework that more directly addresses threat and risks and enables approaches to more quickly and proactively address explicit threats. This can be achieved by the application of High Assurance Security Evaluation and Trusted Delivery methodology to all vendors and networks. The implementation of genuine end-to-end encryption solutions would also be critical.

(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?*

Regarding government contracting opportunities relating to delivering 5G networking solutions, the contract award evaluation criteria should promote the selection of US vendors who are embedding dramatic security and threat mitigation approaches into their offerings. This would seriously incentivize US technology developers to invest in secure 5G technology development.

(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?*

As discussed above, implementation of High Assurance Evaluation and Trusted Delivery offer the most immediately available high impact solutions in this regard.

(6) *What other actions should the US Government take to fulfill the policy goals outlined in the Act and the Strategy?*

To better ensure the security, reliability, and trustworthiness of our 5G infrastructure the US should establish an enduring framework that focuses on development of methods and solutions that more directly mitigate threats and that deliver a focus on direct threat mitigation across the entire deployment lifecycle of 5G (and beyond) communications solutions.