CSR C

Communications Security, Reliability and Interoperability Council

September 2018

Working Group 3

Network Reliability and Security Risk Reduction

**ADDENDUM to Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks**

Table of Contents

10 Final CSRIC Recommendations for the FCC 3

10.5 Recommendations for Supply Chain 3

10.5.1 Regulatory Action 3

10.5.2 Support NIST CSF Update to Supply Chain Procedures 3

10.5.3 Close Collaboration with DHS ICT and NIST 3

11 Final CSRIC Recommendations for Industry 4

11.5 Recommendations for Supply Chain 4

11.5.1 Collaboration with DHS 4

11.5.2 Supply Chain Risk Management 4

11.5.3 Evaluation of Supply Chain Risks 4

# 10 Final CSRIC Recommendations for the FCC

## Recommendations for Supply Chain

The CSRIC makes the following Supply Chain recommendations for the FCC:

### Regulatory Action

The supply chain is a free market driven partnership between numerous companies globally. Restrictions on suppliers in the communication ecosystem, or any industry ecosystem for that matter, can have unintended consequences that need to be fully understood. If the FCC decides that regulatory action on SCRM is necessary based on responses to the current NPRM on restricting use of USF Funds, that regulatory action should be focused as narrowly as possible to avoid broader impacts across the supply chain. The working group recommends the Commission fully consider the ongoing work within the DHS and NIST prior to taking any actions.

### 10.5.2 Support NIST CSF Update to Supply Chain Procedures

CSRIC recognizes that Supply Chain best practices are well documented by a number of different industry standards bodies – NIST, COBIT, ISO to name a few. CSRIC recommends that the FCC support the NIST collaborative process to define the voluntary procedures and identify the informed references for inclusion in updates to the Cyber Security Framework.

### 10.5.3 Close Collaboration with DHS ICT and NIST

Currently, DHS is driving multiple working groups focused on identification of critical infrastructure risk factors and supply chain risk management under the guidance of the National Risk Management Center. These include a comprehensive supply chain threat assessment beginning with the tri-sector (Communications, Information Technology, and Energy) community and the ICT SCRM Task Force. In addition, NIST is currently executing an effort to review and enhance supply chain best practices for inclusion into the cyber security framework.

Supply Chain Risk Management is an incredibly complex activity due to the broad scope of suppliers and technologies in the communications ecosystem. The FCC, other government agencies and even legislators should allow the current public/private partnerships assessing SCRM to complete their assessments so they that can inform the future discussion of potential regulatory actions. We strongly advocate FCC participation in the ICT SCRM Task Force to ensure the best possible flow of information between the diverse Government participants, Industry, and the FCC that can guide next steps in improving SCRM.

# 11 Final CSRIC Recommendations for Industry

## 11.5 Recommendations for Supply Chain

The CSRIC makes the following Supply Chain recommendations for industry:

### Collaboration with DHS

CSRIC recommends industry work closely with DHS to monitor and identify potential threats introduced through supply chain. Specifically, Industry should actively participate in and support the development of recommendations by the DHS Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force in support of the National Risk Management Center.

### 11.5.2 Supply Chain Risk Management

CSRIC recommends all industry members implement a supply chain risk management policy to manage supply chain relationships. Industry should be aware of any potential threats introduced through the supply chain and mitigate those threats according to the risk they pose based on industry specific threat assessment and consistent with an organization’s risk tolerance. It is further recommended that industry consider utilization of Distributed Ledger Technology within their process to address various SCRM activities including proof of ownership, traceability, and transparency and to facilitate the sharing of this information in a verifiable manner.

### 11.5.3 Evaluation of Supply Chain Risks

The CSRIC recommends that industry consider using the NIST National Vulnerability Database (NVD), including Common Vulnerability and Exposures (CVE) and the Common Vulnerability Scoring System (CVSS), to characterize, categorize, and score vulnerabilities in the supply chain.

Industry includes the suppliers who should be using these resources as part of their development cycle on a regular basis.