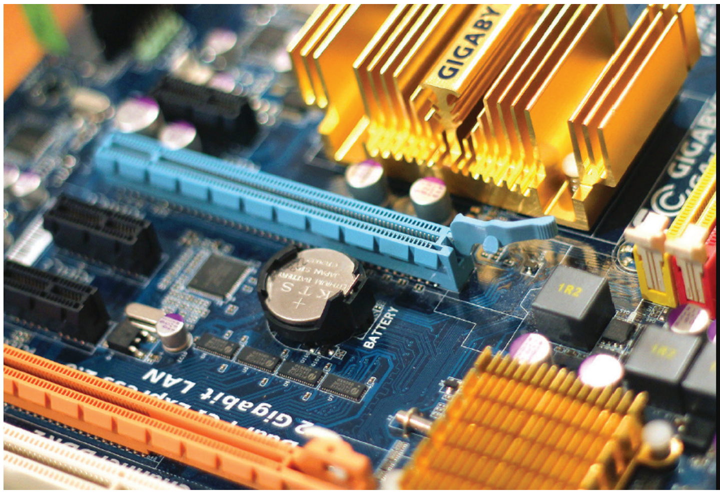

NATIONAL SUPPLY CHAIN INTEGRITY MONTH

INFORMATION AND COMMUNICATIONS TECHNOLOGY

National Counterintelligence and Security Center Factsheet

April 2021

Information and Communications Technology (ICT) supply chain risk management (SCRM) is the process of identifying and mitigating risks in the manufacture and distribution of ICT products and services. While the Information Technology (IT) sector and the Communications sector face different supply chain risks, their mitigation strategies are similar. Both sectors emphasize having an end-to-end Cyber-SCRM program, continuously evaluating risks to vendor networks, and maintaining geographically-diverse and occasionally-redundant supply chains in the event of a manufacturer compromise. The following highlights some common risks and best practices for both sectors. For additional SCRM information, please visit **www.NCSC.gov.**

Risks to IT Sector

- Software supply chain vulnerabilities
- Large-scale denial of service attacks on Domain Name System (DNS) infrastructure
- Disruption of e-Commerce activities
- Weak intrusion detection capabilities

Best Practices for the IT Sector

- Use effective security metrics to demonstrate implementation of good security controls
- Standardize approach to hardware manufacturing when possible
- Regularly evaluate Cyber-SCRM security priorities
- Monitor metrics from the field
- Establish a supply chain incident management team
- Participate in public-private partnership
- Promote security-conscious culture and promote basic cyber hygiene

Risks to Communications Sector

- Software supply chain vulnerabilities
- All Hazards including Natural disasters and extreme weather
- Global political and social disruptions
- Cyber vulnerabilities

Best Practices for the Communications Sector

- Establish joint design and manufacturing partners
- Use Company-owned facilities for in-house manufacturing
- Prioritize critical assets to optimize protections against supply chain risks
- Maintain geographically-diverse and sometimes redundant supply chain operations
- Keep sufficient inventory on hand to recover from major events
- Dedicate a SCRM program for software products
- Assess risks to vendor ecosystem

NOTE: Information contained herein was gathered from the most reliable sources found in the public domain on supply chain risk management, including information from the Department of Homeland Security, the National Institute of Science and Technology, the Federal Bureau of Investigation, and the National Counterintelligence and Security Center.

The information on this product was prepared with the assistance of the 2021 Federal Virtual Intern Service