crowell moring

CLIENT ALERT

Draft NIST Guidance Highlights Supply Chain Fundamentals as Key Practices in Cyber Supply Chain Risk Management

Feb.21.2020

Last week, the National Institute of Standards and Technology (NIST) published the draft NISTIR 8276 "Key Practices in Cyber Supply Chain Risk Management" providing Key Practices and related recommendations for monitoring, controlling, and understanding how to conduct cyber – supply chain risk management (C-SCRM). The Eight Key Practices are general and apply equally, in practice, to both traditional supply chain management and C-SCRM, including:

- Integrating SCRM across the organization,
- Understanding the organization's supply chain, and
- Assessing and monitoring SCRM throughout the supplier relationship.

Specific guidance includes, among others:

- Increasing Board involvement in C-SCRM;
- Understanding the cyber relationship with suppliers, including whether they process critical data; and
- Using third-party assessments to evaluate suppliers.

The guidance should serve to remind organizations of the need to know their supply chain well and to have a purposeful approach to its management. Organizations have an opportunity to comment on this draft guidance until March 4, 2020.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Stephanie L. Crawford
Associate – Washington, D.C.
Phone: +1 202.624.2811
Email: scrawford@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com