ROGERS | JOSEPH | O'DONNELL

rjo.com

CYBER & SUPPLY CHAIN SECURITY

Federal government contractors face challenging cyber and supply chain security obligations. Laws, regulations and contract requirements obligate federal contractors to improve cybersecurity practices and reduce risk throughout the supply chain. Federal scrutiny of contractor cyber and supply chain measures is increasing. The Department of Defense intends to assess security as a means to determine eligibility for new contracts and will use demonstrated security as a competitive discriminator in acquisitions. RJO can assist.

Requirements You Should Know

Defense contractors are required to have "adequate security" to protect all forms of Covered Defense Information (CDI) relying upon the 110 safeguards of NIST SP 800-171. Recent events have focused the attention of Congress, DoD and other federal agencies upon the continuing vulnerability of the U.S. industrial base to economic espionage and other forms of cyber and supply chain intrusion. No longer will it be sufficient for companies to take minimum measures to protect against cyber attacks and secure their supply chains.

DoD can be expected to enforce the cyber DFARS requirements and to review the System Security Plans (SSPs) and Plans of Action and Milestones (POAMs) of its contractors. Companies with inadequate security may be excluded from bidding. Those with superior superiority likely will gain evaluation advantage in competitive procurements. Failure to deliver on promised security will expose companies to review and possible contract liability.

What is Needed

We recommend federal contractors combine means to document compliance as well as demonstrate security achievements – doing so both satisfies risk management concerns (to mitigate potential liability) and serves business capture objectives (through positive competitive discriminators).

Our Credentials

RJO has distinct credentials to assist with the compliance and business objectives. Our security practice is led by Bob Metzger, nationally recognized as a leading subject matter expert in cyber and supply chain security and government contract law. Named a 2016 "Federal 100" awardee, *Federal Computer Week* cited Bob for his "ability to integrate policy, regulation and technology." Chambers USA (2018) ranks Bob among top government contracts lawyers and said that "[h]e is particularly noted for his expertise in cyber and supply-chain security with clients regarding him as the 'preeminent expert in cybersecurity regulations and how they affect government contractors.'" You can review his cyber and supply chain publications here. RJO, a boutique firm that has specialized in public contracts for more than 35 years, is placed in Band 2 by The Legal 500 (2018) and in Tier 2 by Chambers USA (2018) – the only boutique ranked in the top two tiers.

Our expertise encompasses security of information and information systems, network security, cloud computing, operational technology, the Internet of Things (IoT), and a breadth of supply chain issues such as counterfeit parts prevention, trusted sources and parts pedigree and provenance. Many of our lawyers have SECRET clearance and one has a TS/SCI clearance. We have experience in advising foreign owned companies and with export controls.

Our Approach

We leverage industry-leading expertise and deep understanding of government objectives to save you time and money by focusing on what matters, and telling you what doesn't. We understand that security is a process and we will work with you to identify what can be realized in the near-term and plan what will take longer. We know that security has a cost and we seek to help you realize a return on your security investment.

We work with your internal resources to maximize their involvement and contribution. We do work that is appropriate for lawyers and recommend other specialists where they provide needed expertise. We have established working relationships with many government entities and resources. We capitalize on our experience in assisting companies of many different sizes and product/service focus. Where appropriate, our assessments are subject to the attorney-client privilege. Where requested, we can deal directly with government officials with you or on your behalf. Our team is highly accomplished in bid protest litigation, and we can defend or assert your interests in civil litigation or administrative proceedings.

Our Cyber & Supply Chain Services

Risk Assessment	Considering your products and services, and present state of security, we can assist you to in preparing a risk-based assessment of your cyber and supply chain security. We can help you identify gaps and prioritize measures to respond and mitigate.
Security Strategy	Considering risk factors and your business circumstances, we can help you to fashion and document a time-phased security strategy to guide enterprise actions.
Compliance Review	We can conduct efficient review of your compliance status, using our knowledge of cyber and supply chain contract requirements and federal oversight and administration. This can prove crucial in preparing for government assessment of your security.
Demonstration & Documentation	As the government moves away from a trust-based approach to security, we can work with you on demonstration and documentation of your security accomplishments.
Application & Interpretation	Key federal requirements, such as the -7012 DFARS, often raise difficult questions of application and interpretation. We can advise, document and support your decisions.
Contract Terms & Flowdown	We can assess and advise on recurring and tailored solicitation and contract terms and help you to address issue that arise with mandatory flowdown and vendor adherence.
Policies & Procedures	Our extensive experience enables us to aid in preparation of policies and procedures that will guide you internal resources on responsibilities and continuing compliance.
Training	We regularly present and train on cyber and supply chain matters.
Incident Response	When you suspect a cyber incident, we can advise on incident response requirements and assist in the event of subsequent government review.
Competition Matters	We have advised leading companies on how to respond to RFIs and solicitations with cyber and supply chain requirements in order to assure fair competitive opportunity.
Bid Protests	RJO's bid protest practice is recognized as among the best in this practice area and we have a long track record of success at the GAO and Court of Federal Claims.
Investigations & Defense	Led by Brian Miller, we combine the benefits of past government experience with high-level subject area expertise to help respond to cyber/supply chain investigations.
Corrective Measures	If adverse experience dictates new measures to improve cyber and supply chain security, we have the expertise and relationships to assist in design and decision.

Your Next Step

Even the most sophisticated companies find it challenging to know how to respond to evolving threats, newly discovered vulnerabilities and increasing Government demands. We'd be pleased to schedule an initial, complimentary consultation. Contact Bob Metzger directly at (202) 777-8951 or rmetzger@rjo.com.

Our Core Team

Robert S. Metzger (DC) - a nationally recognized expert with years of experience in cyber and supply chain counseling and controversy advice.

Brian D. Miller (DC) - joined RJO after a distinguished government career that included 10 years as GSA Inspector General and service as a senior federal prosecutor.

Jeffery M. Chiow (DC) – co-chair of RJO's Government Contracts Practice Group and highly regarded for his bid protest expertise and cyber/supply chain knowledge.

Lauren B. Kramer (SF) – San Francisco partner with extensive litigation and trial experience and strong background in cybersecurity regulatory regimes.

Washington, D.C. Office
875 15th Street, NW, Ste 725
Washington, D.C. 20005
202.777.8950

San Francisco, CA Office
311 California Street, 10th Flr.
San Francisco, CA 94104
415.956.2828