# Cybersecurity 2022: What Companies Doing Business with the Government Need to Know - Protecting Sensitive Information and CMMC

08.11.2022

**Thursday, August 11, 2022**
2:00 p.m. - 3:30 p.m. ET

This series, taught by experts in the field, will walk participants through the most important issues facing government contractors as they navigate the fast-changing issues of cybersecurity. Starting with a comprehensive overview of CMMC and key regulations, and ending with a session about how to deal with cyber incidents and breach of your systems, this series will also delve into the new government contracting rules relating to cybersecurity, considerations relating to cloud computing and supply chain issues in light of today's cyber events. This webinar series will combine teaching of the key rules with war stories from the front lines and practical advice from experienced practitioners.

**Townsend L. Bourne** is a partner in the Government Contracts, Investigations & International Trade Practice Group at Sheppard Mullin, and Leader of the Firm's Government Business Group. She represents clients in the aerospace and defense industry as well as commercial companies and cloud service providers. Townsend specializes in matters relating to cybersecurity and data protection for government contractors and is the author of numerous articles relating to cybersecurity and government contracting.

**Dates and Topics**

All sessions run from 2:00 pm to 3:30 pm (ET).

To view all the whole series registration, click here.

1. August 11: Protecting Sensitive Information and CMMC

During this initial class in the series, we will discuss and provide important guidance for government contractors seeking to ensure compliance with the government's rapidly expanding cybersecurity requirements. Contractors will learn about new developments under the Biden Administration's Cybersecurity Executive Order as well as existing statutory and regulatory requirements applicable to contractors. Discussion will cover key agency provisions and definitions (CUI, CDI, NIST, SPRS, etc.) with focus on the defense industrial base (FAR requirements, DFARS Assessments, CMMC), cyber considerations for owners and operators of information technology systems, and best practices for compliance.

2. September 8: Data in the Cloud

This training will explore cyber issues in the cloud, including Federal policies and guidance, acquisition of cloud services, and issues unique to Cloud Service Providers (CSPs). We will examine the Federal Risk and Authorization Management Program (FedRAMP) and related requirements, as well as the processes to obtain FedRAMP authorization. In addition, the class will examine agency-specific approaches to cloud computing, including DoD cloud provisions, and considerations when using a third party to provide cloud services under agency contracts.

3. October 6: Cybersecurity Supply Chain Considerations

This program will discuss cybersecurity requirements with a specific focus on supply chain security and initiatives stemming from the Solar Winds hack and other attacks. We will discuss forthcoming requirements for contractors relating to enhancing software supply chain security as well as emerging issues relating to Internet of Things (IoT) devices. Contractors will learn about current regulations relating to prohibited sources of IT goods and services and similar restrictions they are likely to see in the near future.

4. November 10: Cyber Threat Information Sharing and Incident Reporting, Investigation and Response

This final class in the series will address cyber threats and incident reporting requirements as well as programs for sharing information on cyber. We will delve into existing regulations governing incident response and discuss future developments anticipated in this area. We also will discuss information sharing programs, including recent initiatives by the Cybersecurity & Infrastructure Security Agency (CISA), as well as the risks and benefits associated with participation in such programs. Finally, we will discuss considerations and best practices for incident response.

Click here to learn more and register.

## Attorneys

Townsend L. Bourne

Nikole Snyder

## Practice Areas

Privacy and Cybersecurity