SheppardMullin

Townsend L. Bourne

Partner
2099 Pennsylvania Avenue, N.W.
Suite 100
Washington, DC 20006-6801

T: +1.202.747.2184
F: +1.202.747.3836
tbourne@sheppardmullin.com

Townsend Bourne is a partner in the Governmental Practice in the firm's Washington, D.C. office. She is Leader of the firm's Aerospace, Defense & Government Services Team, and of the Governmental Practice Cybersecurity & Data Protection Team.

Areas of Practice

Townsend is a strategic thinker and advocate for companies that do business with the U.S. Government, either directly or through a prime contractor or reseller. She provides insightful legal counsel and proactive solutions that align with her clients' objectives, including forward-thinking strategies for compliance with evolving cyber and supply chain regulations and standards, as well as risk mitigation.

Noted as a "skilled government cybersecurity attorney" by *Legal 500*, she chairs the Coalition for Government Procurement's Cyber and Supply Chain Security Committee, and is a sought-after speaker, go-to resource, and author on cybersecurity and national security developments affecting companies that interface with the government.

Townsend's expertise lies in navigating the complexities of government regulations and policies, ensuring that companies not only comply with the law but also leverage it to their advantage. She specializes in counseling clients on issues involving cybersecurity, national security, critical infrastructure, supply chain risk management, and emerging technologies, including Department of Defense (DoD) and civilian agency security requirements, NIST, FedRAMP, artificial intelligence (AI), secure software development practices and SBOMs, and incident response. Her experience covers all key industry sectors – aerospace and defense, electronics, information technology, communications, energy, financial services, construction, transportation, and healthcare, as well as international suppliers.

Townsend is equally adept at negotiation of subcontracts and teaming agreements, conducting internal investigations, preparing contractor claims, and litigating disputes arising out of doing business with the government, both in lawsuits involving government agencies directly and in disputes between commercial parties. She is an expert on both the commercial litigation strategies for these disputes and litigating in the specialized forums they are subject to.

Her experience includes the Contract Disputes Act and the False Claims Act, bid protests before the Government Accountability Office and Court of Federal Claims, and claims litigation before the Armed Services Board of Contract Appeals and the Civilian Board of Contract Appeals.

Honors

Best Lawyers: Ones to Watch, *Best Lawyers*, 2026

Leading Lawyer - Government Contracts: Cybersecurity, *Chambers USA*, 2024-2025

Leading Lawyer - Government Contracts, *Chambers USA*, 2025

Aerospace & Defense Editorial Advisory Board, *Law360*, 2023

Recommended Lawyer: Government Contracts, *Legal 500*, 2023-2025

Top Author, *JD Supra* Readers' Choice Awards, 2023-2025

Washington, D.C. Rising Star, *Super Lawyers*, 2019-2020

Experience

Representative Matters

- Represented a Northern Virginia-based multinational professional services and information technology company in a significant bid protest by a competitor over a multi-billion dollar National Security Agency contract for analyst services. The Government Accountability Office rejected the competitor's protest, thus securing the contract award for our client.
- Advised a New York-based designer and manufacturer of electric control systems for aerospace and defense as plaintiff in a contentious case relating to using trade secret and proprietary files stolen from our client. After sanctions being issued against the defendant and an expert witness disqualified, the case was settled and dismissed.
- Advised a large defense contractor and led a forensics investigation relating to several cybersecurity matters to include a sophisticated phishing scam that resulted in a Business Email Compromise, closely coordinating with the FBI, government officials, and other impacted parties regarding investigation and recovery of funds
- Represented a multinational aerospace and defense company with a government contracting data rights matter, advising on contract provisions and negotiation of terms and communications with the government
- Serve as government contracts counsel to a premiere American e-commerce multinational, advising on public sector agreements and compliance with federal law and regulations. Assist with drafting agreements, flow-down provisions, and negotiation of contracts, including negotiation of a multimillion-dollar agreement with a major player in the space industry.
- Represents Fortune 500 government contractor before the U.S. Court of Federal Claims in on-going Contract Disputes Act case involving multiple contractor claims and government counterclaims related to an $874 million contract with the U.S. Postal Service
- Successfully defended large government contractor in False Claims Act dispute before the U.S. District Court for the Eastern District of Virginia
- Represented major contractor before the Civilian Board of Contract Appeals in contract dispute with the Department of the Interior that resulted in favorable settlement for client
- Succeeded in Court of Federal Claims protest to overturn a decision by the Department of Education to cancel a solicitation for critical services
- Represented major international aerospace company before the Armed Services Board of Contract Appeals in data rights dispute with the government that resulted in favorable settlement for client

- Successful prosecution and defense of numerous bid protests before the Government Accountability Office for a variety of clients including large defense contractors and GSA schedule vendors
- Conducted internal investigations for large government contractors and counseled clients regarding resolution of investigations involving mandatory disclosure of contract overpayments and the Procurement Integrity Act
- Assisted in drafting and negotiating key provisions in subcontracts and teaming Agreements for multiple clients, including commercial service providers and value-added resellers

Cybersecurity and Data Protection Experience

- Counsels clients regarding agency-specific cybersecurity and data protection requirements, including DFARS 252.204- 7012, and the Cybersecurity Maturity Model Certification (CMMC) program
- Works with clients to understand the interplay between the above requirements and rules specific to cloud service providers, including FedRAMP and the DoD Security Requirements Guide
- Assists clients with creation and finalization of System Security Plans, Incident Response Plans and Insider Threat Plans
- Helps with drafting and negotiation of subcontract and vendor provisions relating to data security
- Counsels clients with regard to supply chain risk management (SCRM), including secure software development (SBOMs and SSDF), prohibited sources (e.g., Section 889), and security of Internet of Things (IoT) devices
- Develops client and industry-specific cybersecurity compliance framework and training materials addressing obligations and best practices for handling sensitive information (including Controlled Unclassified Information (CUI)), data protection, and incident response
- Leads incident response and determination of reporting obligations, including communications with the Defense Industrial Base (DIB) pursuant to DFARS 252.204-7012, law enforcement, customers, and other government agencies

Articles

- What Compliance Leaders Need to Know Ahead of Crucial DOJ Data Security Program Deadline
  Corporate Compliance Insights, 09.08.2025
- Eye on Privacy: 2024 Year in Review
  01.21.2025
- Governmental Practice Cybersecurity and Data Protection: 2024 Recap & 2025 Forecast Alert
  01.07.2025
- 4 Ways To Prepare For DOD Cyber Certification Rule
  Law360, 09.30.2024
- What Government Contractors Need to Know About Artificial Intelligence Legal Issues
  ABA Procurement Lawyer, 07.29.2024
- Legal Corner: Data, Deals, and Diplomacy: How the Bulk Data Executive Order Will Shape Future Contracts and Security Practices
  The Coalition For Government Procurement, 07.12.2024

- A Break Down of the Proposed CIRCIA Rule
  Federal News Network, 06.05.2024
- Updates on Greenhouse Gas Emission Disclosure Requirements for Defense Contractors
  Westlaw Today, 04.23.2024
- Governmental Practice Cybersecurity and Data Protection, 2023 Recap & 2024 Forecast Alert
  02.08.2024
- Eye on Privacy: 2023 Year in Review
  01.26.2024
- FedRamp Modernization & The Draft OMB Memo
  Federal News Network, 12.13.2023
- Unpacking The FAR Council's Cybersecurity Rules Proposal
  Law360, 10.25.2023
- Bracing For Rising Cyber-Related False Claims Act Scrutiny
  Law360, 09.18.2023
- ChatUSG: What Government Contractors Need To Know About AI
  Briefing Papers, 07.2023
- ChatUSG: What government contractors need to know about AI
  Westlaw Today, 05.22.2023
- Eye on Privacy 2021 Year in Review
  01.11.2022
- Securing the Government Supply Chain: Section 889 and Prohibitions on Chinese Telecom
  Procurement Lawyer, Winter 2021
- Legal Corner: What You Need to Know About the President's September 22 “Divisive Ideology” Executive Order
  The Coalition for Government Procurement, 11.06.2020
- Blockchain Tech has Numerous Applications for Defense
  National Defense, 12.2019
- The Long Reach Of Section 889 (aka the Anti-Huawei Rule)
  The Coalition for Government Procurement; Friday Flash, 12.06.2019
- Viewpoint: Some FAQs Answered About the New Cybersecurity Rule
  National Defense, 07.03.2018
- Achieving Cyber-Fitness in 2017: Part 6—Potential Liabilities and Putting It All Together
  The Government Contractor, 12.06.2017
- Achieving Cyber-Fitness in 2017: Part 5—Cyber Incident Reporting and Response
  The Government Contractor, 09.13.2017
- Achieving Cyber-Fitness in 2017: Part 4—Subcontracts, Joint Ventures And Teaming Agreements
  The Government Contractor, 06.14.2017
- Presidential Executive Order on Cybersecurity: No More Antiquated IT
  Bloomberg Law Privacy and Security Law Report, 05.29.2017

- Achieving Cyber-Fitness in 2017: Part 3—Proving Compliance And The Role Of Third-Party Auditors
  The Government Contractor, 04.05.2017
- Achieving Cyber-Fitness in 2017: Part 2—Looking Beyond The FAR And DFARS—Other Safeguarding And Reporting Requirements
  The Government Contractor, 02.22.2017
- Achieving Cyber-Fitness in 2017: Part 1—Planning for Compliance
  The Government Contractor, 02.01.2017
- Lots of Little Things - Recent FAR Updates
  Law360, 08.19.2013
- Authored chapter, "General Overview of Cloud Computing," *Cloud Computing Legal Deskbook,* 2013 Edition, Thomson Reuters Westlaw, 2013

AI Law and Policy Blog Posts

- "AI Considerations in Government Contract-Related M&A Transactions," August 8, 2024
- "Flash Briefing on White House Executive Order on AI Regulation and Policy," November 3, 2023

Blockchain and Cryptocurrency: Law of the Ledger

- "Blockchain and Metaverse Legal Issues for the Government and Government Contractors," May 23, 2022

Global Trade Law Blog Posts

- "Data, Deals, and Diplomacy, Part II: Big Obligations for Big Data," November 4, 2024
- "Commerce Takes on AI: Recent Developments from BIS on AI," October 30, 2024

Government Contracts & Investigations Blog Posts

- "Don't Fall Behind: The CMMC Final Rule to Update the DFARS is Here!," September 15, 2025
- "The Expanding Scope of FCA-Cybersecurity Liability," September 5, 2025
- "Sheppard Mullin's Government Contracts Team Launches Revolutionary FAR Overhaul Tracker," June 12, 2025
- "Trump's New Cybersecurity Executive Order: What Contractors Need to Know," June 10, 2025
- "All American AI: New OMB Memos Set Priorities for Federal AI Use and Acquisition," May 2, 2025
- "FedRAMP 20x – Update on Significant Change Process and Assessment Scope Standards," May 2, 2025
- "FedRAMP 20x – Major Overhaul Announced to Streamline the Security Authorization Process for Government Cloud Offerings," April 2, 2025
- "FedRAMP Releases New Draft Authorization Boundary Guidance," January 29, 2025
- "Data, Deals, and Diplomacy, Part III: DOJ Issues National Security Final Rule with New Data Compliance Obligations for Transactions Involving Countries of Concern," January 29, 2025
- "Looking Beyond FedRAMP – Lessons from the U.S. Treasury Cybersecurity Incident," January 29, 2025

- "At Long Last – The FAR CUI Rule is Here!," January 29, 2025
- "Governmental Practice Cybersecurity and Data Protection: 2024 Recap & 2025 Forecast Alert," January 7, 2025
- "DoD Issues Proposed Rule for New Disclosures on Foreign Review of Computer Code," December 13, 2024
- "Update – Penn State to Pay Up for Cyber-Related FCA Case," October 30, 2024
- "Countdown to Compliance: DoD Finalizes the CMMC Program Rule," October 15, 2024
- "The CMMC Rule To Update the DFARS is Here!" August 16, 2024
- "Navigating the New Cybersecurity Regulatory Landscape Post-Chevron," July 31, 2024
- "Summer Heat Ramping Up: FedRAMP Releases Final OMB Memo and Announces Update on Roadmap Progress, Automation Site Launch, and the Agile Delivery Pilot Launch," July 31, 2024
- "Data, Deals, and Diplomacy: How the Bulk Data Executive Order Will Shape Future Contracts and Security Practices," June 26, 2024
- "Latest Cyber-Related FCA Settlement Underscores the Breadth of DOJ's Civil Cyber-Fraud Focus," June 26, 2024
- "FAR Council Releases Rulemaking on Prohibitions for Semiconductors," June 3, 2024
- "Not an April Fools Joke – FAR Part 40 Final Rule Has Been Published," April 29, 2024
- "Better Safe Than Sorry: OMB Releases Memorandum on Managing AI Risks in the Federal Government," April 29, 2024
- "CISA Cyber Incident Reporting for Critical Infrastructure Will Significantly Impact Government Contractors, Suppliers, and Service Providers," April 8, 2024
- "Updates on GHG Emissions Disclosure Requirements," March 27, 2024
- "CISA Opens Repository for Submission of Software Security Attestation Forms," March 27, 2024
- "Emerging AI Landscape: FedRAMP Publishes Draft Emerging Technology Prioritization Framework in Response to Executive Order on Artificial Intelligence," February 29, 2024
- "Governmental Practice Cybersecurity and Data Protection, 2023 Recap & 2024 Forecast Alert," February 8, 2024
- "For Limited Use Only: Guidance on National Security Delay Determinations under the SEC Cyber Reporting Rule," January 19, 2024
- "DoD IG Report Provides Insight Into Common Missteps When Protecting CUI," January 19, 2024
- "New Year, New Rules: The CMMC Proposed Rule is Here," January 2, 2024
- "Update: CISA Seeks Additional Input from Software Providers on Security Attestation Form," December 6, 2023
- "Time for An Upgrade: OMB Releases Draft Memorandum Modernizing FedRAMP," October 31, 2023
- "Interim Rule Effective in December Establishes Requirements for Contractors to Remove Identified Products and Services from the U.S. Government Supply Chain," October 11, 2023
- "Two New Cybersecurity Proposed Rules Mean Big Changes for Federal Contractors," October 4, 2023

- "Cybersecurity Labeling is (Almost) Here! Biden Administration Announces the U.S. Cyber Trust Mark Program," August 1, 2023
- "White House Provides New Guidance & Extends Deadline for Secure Software Attestations," June 13, 2023
- "NIST Releases Initial Public Draft of NIST SP 800-171, Revision 3 for Protection of Sensitive Government Information," May 24, 2023
- "CISA Releases Proposed Security Attestation Form for Software Producers," May 1, 2023
- "ChatUSG: What Companies Doing Business with the Government Need to Know About Artificial Intelligence," May 1, 2023
- "Reassessed: FedRAMP Releases Revised Obligations and Standards for Cybersecurity Assessors," April 27, 2023
- "Biden Administration Releases Highly Anticipated National Cybersecurity Strategy," March 9, 2023
- "Proposed Rule Requires Contractors to Disclose Greenhouse Gas Emissions and Climate-Related Financial Risk," November 29, 2022
- "Third Time's The Charm – FedRAMP Releases Draft Authorization Boundary Guidance Version 3 for Public Comment," September 28, 2022
- "Federal Government Outlines New Security and Attestation Requirements for Software," September 28, 2022
- "NIST Wants Your Input – Updating NIST's Controlled Unclassified Information (CUI) Guidelines," July 27, 2022
- "Updated Timeline for CMMC Implementation," June 29, 2022
- "Well, That Didn't Take Long – DOJ Announces its First Settlement of a Civil Cyber-Fraud Case," March 10, 2022
- "Seeking HoNIST Opinions, Part II – NIST Invites Comments on Major Revision to Cyber Supply Chain Risk Management Practices and Software Guidelines Mandated By Cybersecurity Executive Order," November 10, 2021
- "DOD Updates Its Cybersecurity Certification Program – CMMC 2.0: What Contractors Need to Know," November 10, 2021
- "DOJ Announces Civil Cyber-Fraud Initiative To Enforce Contractor Cybersecurity Compliance," October 28, 2021
- "Moving to Zero Trust – CISA and OMB Seek Comments on Zero Trust Publications and Cloud Security Technical Reference Architecture under Cybersecurity Executive Order," September 15, 2021
- "Double Time – NIST Seeks Comments on Major Revision to Practices for Developing Cyber-Resilient Systems (SP 800-160) and Assessing Security and Privacy Controls in Information Systems and Organizations (SP 800-53A)," August 30, 2021
- "Watch Your Boundaries – FedRAMP Releases Draft Authorization Boundary Guidance for Public Comment," July 28, 2021
- "At a Glance: White House 100-Day Supply Chain Report," June 29, 2021
- "Right on Time – NIST Releases Definition of "Critical Software" Per Biden's Cybersecurity Executive Order," June 29, 2021
- "Seeking HoNIST Opinions – NIST Invites Comments on Major Revision to Cyber Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161) and Provides Further Software Supply

Chain Guidance," May 26, 2021

- "Biden's Cybersecurity Executive Order," May 17, 2021
- "Finding the Weak Links – President Biden Executive Order Demands Review of Critical U.S. Supply Chains," March 31, 2021
- "Key Provisions You Should Know From FY 2021 NDAA," January 27, 2021
- "The NISPOM is Becoming a Regulation & Contractors Have Six Months to Comply," January 27, 2021
- "IoT Legislation Passes Congress," November 30, 2020
- "DoD's Long Awaited Rule on CMMC – Plus a New Cybersecurity Assessment Methodology for Contractors to Start Right Now," September 29, 2020
- "GSA's Take on Implementation of Section 889," September 29, 2020
- "IoT Legislation Advances in Congress," September 29, 2020
- "Interim Rule Confirms Section 889 Part B Restriction on Contractor Use of Chinese Telecom Will Go Into Effect August 2020," July 14, 2020
- "DOD CMMC Update – Third Party Auditors Gear Up and COTS Providers Get a Pass," May 28, 2020
- "DoD Issues Class Deviation to Address Contractor Reimbursement for Paid Leave Required to Maintain a Mission-Ready Workforce During the COVID-19 Outbreak Pursuant to Section 3610 of the CARES Act," April 10, 2020
- "Presidential Executive Orders Delegate Additional Authorities To Respond To COVID-19 Outbreak," April 1, 2020
- "Presidential Executive Order Calls on HHS to Issue Priority Contracts and Allocate Scarce Medical Resources," March 20, 2020
- "The True Impact of the Chinese Telecom Ban on Government Contractors," November 25, 2019
- "GSA Implements Restrictions on Certain Chinese-Made Telecommunications Services and Equipment," September 27, 2019
- "Effective Last Month! – DoD's Implementation of New FAR Prohibitions on Chinese Telecommunications Equipment and Services in Government Contracts," September 5, 2019
- "Effective Immediately! – FAR Amended to Include Prohibition on Chinese Telecommunications Equipment and Services in Government Contracts," August 13, 2019
- "Cyber Update: DoD Contractor Cybersecurity Certification and 33 New Enhanced Controls to Combat the Advanced Persistent Threat," June 26, 2019
- "New Executive Order To Further Restrict Business with Huawei and Other Foreign Adversaries Engaged in Cyber Espionage," May 20, 2019
- "'Internet of Things' Guidance to be Added to Cybersecurity Requirements for Agencies and Federal Contractors," April 29, 2019
- "More Opportunities On the Horizon for Small Businesses Seeking to Sell Cloud Computing to the Government," February 27, 2019
- "Recovering After the Shutdown: Proposed Legislation to Guarantee Back Pay for Government Contractors," February 1, 2019

Eye on Privacy Blog Posts

- "Leveling Up: Will CMMC Contract Obligations Impact Your Organization?," October 16, 2025
- "DOJ Announces 90-Day Grace Period for Companies to Comply with New Data Security Rules on Foreign Adversary Access to U.S. Sensitive Data," April 16, 2025
- "'All Hands on Deck' – White House Continues to Call on Agencies for AI National Security Plan," December 16, 2024
- "Countdown to Compliance: The Department of Defense Finalizes Its Cybersecurity Program Rule," October 25, 2024
- "New Program Under Biden Executive Order to Prevent Access to American's Sensitive Personal Data by Foreign Actors," April 24, 2024
- "NIST Expands Cybersecurity Framework with Release of Version 2.0," March 18, 2024
- "Defense Department Outlines Its Future Cybersecurity Program," January 25, 2024
- "Cybersecurity Labeling Program to Increase Transparency of IoT Device Security," August 3, 2023
- "NIST Seeks Input on Standards for Protecting Sensitive Government Information," June 15, 2023
- "Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Five- Further Adoption of FedRAMP & StateRAMP," January 25, 2023
- "Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Four – Cybersecurity Federal Acquisition Regulation (FAR) Updates," January 24, 2023
- "Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Three – Secure Software Development Attestation Requirements," January 23, 2023
- "Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part Two – NIST SP 800-171, Revision 3," January 19, 2023
- "Do Business With the Federal Government? Here's a 2022 Cybersecurity Recap: Part One – CMMC Developments," January 18, 2023
- "White House Aims for Spring 2023 Rollout of Internet of Things Labeling Program," October 28, 2022
- "CISA Seeking Input on Cyber Incident Reporting for Critical Infrastructure," September 26, 2022
- "Updated Timeline for DoD's Cybersecurity Certification Program," June 23, 2022
- "Cybersecurity Act Signed Into Law Creates New Reporting Obligations," March 29, 2022
- "NIST Releases New Guidance on Software Security and Cybersecurity Consumer Labeling Programs," March 14, 2022
- "NIST Seeks Comments on Cybersecurity Framework Refresh," March 10, 2022
- "White House Focuses on Improving the Cybersecurity of National Security Systems," February 15, 2022
- "2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 4 of 4: Cybersecurity Maturity Model Certification ("CMMC") 2.0," December 22, 2021
- "2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 3 of 4: Cyber Incident & Ransomware Payment Reporting Legislation," December 21, 2021
- "2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 2 of 4: Department of Justice (DOJ) Civil-Cyber Fraud Initiative," December 20, 2021

- "2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 1 of 4: Biden's Cybersecurity Executive Order (EO 14028)," December 17, 2021
- "Updates Announced to Department of Defense Cybersecurity Certification Program," November 10, 2021
- "NIST Finalizes Guidance on Security and Privacy Control Baselines – SP 800-53B," November 6, 2020
- "Interim Rule Solidifies Cybersecurity Requirements for Defense Industrial Base," October 9, 2020
- "NIST Issues Long-Awaited Final Guidance on Security and Privacy Controls – SP 800-53," October 5, 2020
- "NIST Issues Draft Guidance on Security and Privacy Control Baselines – SP 800-53B," August 6, 2020
- "NIST Proposes Draft Enhanced Security Requirements for Protecting CUI," July 28, 2020
- "NIST Releases Cybersecurity Guidance for Manufacturers of IoT Devices," June 18, 2020
- "CMMC Version 1.0: Enhancing DOD's Supply Chain Cybersecurity," February 12, 2020
- "CISA Releases "Cyber Essentials" to Assist Small Businesses," November 12, 2019
- "Feds Want New IoT Guidance to Address Security Vulnerabilities," May 22, 2019
- "Year In Review: Eye on Privacy 2018," January 28, 2019
- "When the U.S. Government Declares Companies Cyber-Insecure, We Should All Pay Attention," January 7, 2019

Labor and Employment Law Blog Posts

- "Recovering After the Shutdown: Proposed Legislation to Guarantee Back Pay for Government Contractors," January 25, 2019

Organizational Integrity Group Blog Posts

- "Cybersecurity Incident Response," March 22, 2023
- "Ethics & Compliance: Let's Talk About Cybersecurity," February 1, 2023

White Collar & Government Enforcement Blog Posts

- "DOJ's 90-Day Data Security Compliance Grace Period is Over: Are You Compliant?," July 14, 2025
- "DOJ Sues Georgia Tech Entities for Cybersecurity Failures in the Latest Civil Cyber Fraud Initiative (CCFI) Activity," August 23, 2024
- "Update – DOJ Declines to Intervene in Penn State Cyber-Related FCA Case," October 2, 2023
- "Recent Cyber-Related False Claims Act Activity Signals Contractors and Universities Should Examine Their Cybersecurity Practices and Brace for an Uptick in Enforcement," September 11, 2023

Media Mentions

2025 reshaped federal cybersecurity, from new mandates to tougher compliance rules
Federal News Network, 12.22.2025

Today's the day to be in compliance with a data security rule from the Department of Justice
Federal News Network, 07.08.2025

New Proposal For Controlled Information Not Entirely Realistic
Law360, 01.16.2025

Gov't Contracts Policies To Watch In 2025
Law360, 01.01.2025

Artificial Intelligence Poses Legal Threats to Government Contractors
Federal News Network, 08.08.2024

Biden's AI Guidance For Gov't May Need More Risk Controls
Law360, 05.03.2024

Get ready for that proposed rule on defense contractor cybersecurity
Federal Drive, 03.06.2024

Top Government Contracting Policies of 2023: Year In Review
Law360, 12.19.2023

Uncertainties In Cloud Security Update May Deter Contractors
Law360, 11.03.2023

The FAR Council Goes Big into Proposing New Cybersecurity Rules
Federal News Network, 10.10.2023

Navigating Cybersecurity Maturity Model Certification (CMMC) 2.0
SME, 02.09.2023

Sheppard Mullin Forms Broad Gov't Contracts Biz Group
Law360, 01.18.2022

1-in-5 Fortune 500 Companies Still Use Risky Chinese Tech After U.S. Ban
Fortune, 11.24.2020

Tech Firms Support Huawei Restriction, Balk at Cost
E-Commerce Times, 10.22.2020

Agencies, Firms Explore Applications for Blockchain Tech
ExecutiveBiz, 12.12.2019

Huawei Ban's Compliance Rules Too Taxing For Contractors
Law360, 11.01.2019

ABA Section Flags Problems With DFARS/NIST Cybersecurity Guidance
The Government Contractor, 06.13.2018

Speaking Engagements

Presenter, "Recap of the 2024 Federal Procurement Institute: What Did We Learn?" American Bar Association, May 17, 2024

Presenter, "2022 Fall Conference - Expectations for Gov Fiscal Year 2023," The Coalition for Government Procurement, November 16, 2022

Presenter, "Cybersecurity & IT," PubK's Public Contracts Annual Review, January 25-28, 2021

Presenter, "Cybersecurity Compliance Frameworks for Government Contracting," National Contract Management Association's Government Contract Management Symposium, Hyatt Regency Crystal City, Arlington, Virginia, December 3, 2018

Presenter, "FedRAMP and the Cloud; Cybersecurity Update," Ingram Micro Federal Summit, Gaylord National Resort and Convention Center, National Harbor, Maryland, October 31, 2018

"FREE Popular Topics Webinar Series: DoD Cybersecurity Requirements," Public Contracting Institute, August 23, 2018

Events

Pub K's Annual Review 2026
Cybersecurity
02.11.2026

Cyber Year In Review
Webinar, 12.03.2025

ACC NCR: Protecting Data, Avoiding Liability: Navigating DOJ's Cybersecurity Initiatives
In-Person at Sheppard Mullin's Washington DC Office or Via Webcast, 11.05.2025

All-Member Meeting: Cyber Update
Webinar, 08.28.2025

Pub K Annual Review
Cybersecurity
Washington, D.C., 02.12.2025

Fall Training Conference
Cybersecurity, Cloud, & AI Panel: What's Next for the Federal Market?
Falls Church, VA, 11.20.2024

Managing AI Legal Governance Panel
Sheppard Mullin, Washington DC, 11.13.2024

The Inevitable Intrusion: A Legal Guide to Surviving Cyber Incidents
Webinar, 10.15.2024

Cyber Symposium: The Cyber Side Chat
The Black, White, and Grey of Cybersecurity Compliance
Washington, D.C., 09.12.2024

What Companies Need to Know about CMMC–Where We Are, Where We've Been, and Where (We Think) We're Headed
Webinar, 08.28.2024

ACC NCR: Government Contracting Cybersecurity Conference
Who's Afraid of the Big Bad Wolf: The Latest on Cybersecurity Regulatory Updates
04.16.2024

2024 Federal Procurement Institute
Recent Developments in Cybersecurity: On the Front Lines
Graduate Annapolis, 03.08.2024

The White House Executive Order on AI and its Impact on Government Contractors
02.20.2024

Government Contracts Annual Review 2024
Cybersecurity and Data Privacy
Ronald Reagan International Trade Center, Washington, D.C., 02.13.2024

What Contractors Need to Know about the CMMC Proposed Rule
02.05.2024

Flash Briefing on White House Executive Order on AI Regulation and Policy
Webinar, 11.02.2023

Cybersecurity and Government Business – What Government Contractors and Suppliers Should Be Doing Now and What They Can Expect in Cyber and Supply Chain Risk Management
10.11.2023

Tools and Ideas for Asymmetric Advantage: An Executive Perspective
09.26.2023

Defend Your Data – How to Navigate Information and Cybersecurity Requirements to Secure a Place in the U.S. Supply Chain
Storgatan 5, Stockholm, 09.07.2023

2023 Spring Conference - Procurement Watchwords for 2023
Cybersecurity Panel
Falls Church, Virginia, 05.02.2023

PubK's GovCon Annual Review Conference 2023
01.10.2023

Cybersecurity 2022: What Companies Doing Business with the Government Need to Know - Protecting Sensitive Information and CMMC
08.11.2022

Privacy + Security Forum
Developments in Data Security and Incident Reporting for Companies Doing Business with the U.S. Government
Virtual, 03.24.2022

Pub K Annual Review 2022
Cybersecurity and Information Technology Panel
01.25.2022

ACC NCR Cybersecurity Maturity Model Certification (CMMC) and Cybersecurity for Government Contractors – The Current Landscape, What's Coming, and What You Should Be Doing To Prepare
Virtual, 10.14.2021

Cybersecurity 2021: Breach Investigation and Response
Public Contracting Institute
Virtual, 06.17.2021

Cybersecurity 2021: Confronting the Threat - Sharing Information and Spreading the Risk
Public Contracting Institute
Virtual, 05.20.2021

Pub K's Government Contracts Annual Review
Virtual, 01.26.2021

While you Were Social Distancing: Recent Developments in Commercial Item Contracting
Association of Corporate Counsel
12.10.2020

GovCon Cybersecurity Maturity Model Certification ("CMMC") Program
11.19.2020

The Aerospace & Defense Forum: The Evolving National Security Innovation Space for All
Webinar, 09.22.2020

Cybersecurity Landscape Updates
The Coalition For Government Procurement Webinar
07.30.2020

Part Two of the Federal Contractor's COVID-19 Survival Guide
04.02.2020

Webinar - Government Use of Blockchain: What Government Contractors Need to Know
via GlobalMeet, 11.13.2019

Advanced Employment Issues in Government Contracting
06.19.2019

The Coalition for Government Procurement's 2019 Spring Training Conference
05.16.2019

2019 Ingram Micro Federal Summit
04.29.2019

Cybersecurity 2019: Regulations and Standards
Public Contracting Institute
03.13.2019

Cybersecurity 2019: Protecting Sensitive Information
Public Contracting Institute
02.19.2019

Cybersecurity 2019: Introduction and Overview
01.15.2019

Cybersecurity Compliance Frameworks for Government Contracting
Government Contract Management Symposium
12.03.2018

FedRAMP and the Cloud; Cybersecurity Update
Ingram Micro Federal Summit
10.31.2018

FREE Popular Topics Webinar Series: DoD Cybersecurity Requirements
Public Contracting Institute
08.23.2018

Breach Investigation and Response Virtual Class
Cybersecurity: It Isn't Just for Techies Anymore!
Virtual Class, 03.20.2018

Confronting the Threat – Sharing Information and Spreading the Risk Virtual Class
Cybersecurity: It Isn't Just for Techies Anymore!
Virtual Class, 02.20.2018

The Cloud and FedRAMP Virtual Class
Cybersecurity: It Isn't Just for Techies Anymore!
Virtual Class, 01.30.2018

Memberships

Member, State Bar of Virginia

Member, Bar of the District of Columbia

Member, American Bar Association, Section of Public Contract Law

Member, National Defense Industrial Association

Member, U.S. Court of Federal Claims

Member, U.S. Court of Appeals for the Federal Circuit

Podcasts & Webinars

The Inevitable Intrusion: A Legal Guide to Surviving Cyber Incidents
10.15.2024

Flash Briefing on White House Executive Order on AI Regulation and Policy
11.02.2023

Nota Bene Episode 39: Doing Business with the U.S. Government in an Era of Cybersecurity, Espionage and Executive Orders with Townsend Bourne
06.11.2019

Client Testimonials

"Townsend is fantastic on cybersecurity issues in government contracting." – GovCon Client, *Chambers USA*, 2024

“Townsend is a great lawyer to work with. She is thorough and practical, and helped us distill a large amount of complex information into an understandable and workable action plan.” – GovCon Client, *Chambers USA*, 2024

"She's my go-to person for questions relating to cybersecurity. It's a constantly developing area. She provides an action plan, which shows a real understanding of our business, but also of the law too." – GovCon Client, *Chambers USA*, 2024

“Townsend and her team are incredibly responsive and understand our needs and the way our company works….This translates into helpful and practical solutions for us.” – GovCon Client, *Chambers USA*, 2024

"She's a pleasure to work with, and I appreciate her ability to quickly understand the complexities of my business." – GovCon Client, *Chambers USA*, 2024

“Townsend Bourne's specialty in cybersecurity and [other areas] far exceeds my knowledge base." – GovCon Client, *Chambers USA*, 2024

“She's fantastic on [specific issues] in government contracts.” – GovCon Client, *Chambers USA*, 2024

“She was great, responsive, patient and thorough with answering questions." – GovCon Client, *Chambers USA*, 2024

“Townsend Bourne is establishing herself as a true leader in the government cybersecurity space, which is increasingly important.” – GovCon Client - *Legal 500 US*, 2024

**Nothing on this site predicts or guarantees future results.*

Practices

Governmental

Bid Protests
Claims
Contract Cost Accounting
False Claims Act
Foreign Corrupt Practices Act (FCPA)
Intellectual Property Rights Under Government Contracts
Exports and Export-Related Controls
GSA Multiple Award Schedule Contracting
Litigation
Privacy and Cybersecurity
Cybersecurity & Data Protection
Government Contracts
Immigration Investigations and Compliance
National Security
Supply Chain Management

Industries

Aerospace, Defense & Government Services
Artificial Intelligence
Semiconductors

Education

J.D., George Mason University School of Law, 2009, *cum laude*, Notes Editor, *George Mason Law Review*
B.A., Vanderbilt University, 2006, *summa cum laude*

Admissions

Commonwealth of Virginia
District of Columbia
U.S. District Court for the Eastern District of Virginia
U.S. Court of Appeals for the Federal Circuit
U.S. Court of Federal Claims