*This is your Release #1 (April 2026)*

# Cybersecurity

## *A Practical Guide to the Law of Cyber Risk*

### *Second Edition*

**Edited by**
**Edward R. McNicholas & Frances E. Faircloth**

*Cybersecurity: A Practical Guide to the Law of Cyber Risk* is a comprehensive reference on the laws and regulations that govern information security in the United States and abroad and the strategies that can be used to mitigate cyber risks. The book details: sources of cybersecurity law in the United States, including federal and state legislation, executive orders, key court decisions, and agency policies, guidelines and regulations; risk management tools, including insurance, incident response plans, due diligence strategies, and an understanding of the risks arising from the use of artificial intelligence and other developing technologies; sector-specific regulations, such as finance, healthcare, professional services, communications, energy, and others; and cybersecurity laws around the world, including the EU, Canada, China, India, and other nations. The editors have collected the perspectives of leading attorneys in the field, providing comprehensive coverage and analysis, practical tips, forms, checklists, and real-world examples.

New developments added to this release include:

**National cybersecurity policy** has been affected by executive action, including the Trump Administration's revocation of numerous Biden-era executive orders; amendment of E.O. 14144 to reduce compliance burdens; and establishment of a regulatory framework for controlling access to bulk sensitive personal and government-related data, resulting in the Department of Justice's Data Security Program. *Chapter 4, Executive Orders and Related Actions*.

In April 2025, **NIST finalized revised guidance** on cybersecurity incident response risk management practices. Last updated in 2012, the scope of the guidance has changed significantly to reflect the new incident response risk landscape and to align with the Cybersecurity Framework. *Chapter 8, The NIST Cybersecurity Framework*.

The Office for Civil Rights has proposed updates to the Security Rule aimed at strengthening cybersecurity for **electronic protected health information**

*(continued on reverse)*

Practising Law Institute
1177 Avenue of the Americas
New York, NY 10036
**#447969**

(ePHI). The proposal has prompted significant feedback. *Chapter 17, Cybersecurity in Healthcare and Medical Devices*.

In January 2025, the FAR Council proposed a long-awaited **FAR Controlled Unclassified Information (CUI) rule**, aiming to establish uniform requirements for handling CUI across federal solicitations and contracts. The proposed rule also expands the scope of companies subject to CUI protection requirements. *Chapter 18, Federal Contractor Cybersecurity*.

In addition, chapters on the **cybersecurity laws of other nations**, including China, India, Canada, Brazil, Turkey, and others, are updated to reflect the most recent changes. *Part IV, Global Cybersecurity Law*.

Thank you for purchasing *Cybersecurity: A Practical Guide to the Law of Cyber Risk*. If you have questions about this product, or would like information on our other products, please contact customer service at info@pli.edu or (800) 260-4PLI.

# FILING INSTRUCTIONS

# Cybersecurity

## *A Practical Guide to the Law of Cyber Risk*

### *Second Edition*

**Release #1**
**(April 2026)**

| Remove Old Pages Numbered: | Insert New Pages Numbered: |
|---|---|
| ❑ Title page to 9-37 | ❑ Title page to 9-43 |
| ❑ 13-1 to 13-37 | ❑ 13-1 to 13-38 |
| ❑ 16-1 to 18-45 | ❑ 16-1 to 18-49 |
| ❑ 21-1 to 23-51 | ❑ 21-1 to 23-55 |
| ❑ 25-1 to 25-10 | ❑ 25-1 to 25-14 |
| ❑ 30-1 to 34-35 | ❑ 30-1 to 34-37 |
| ❑ I-1 to I-62 | ❑ I-1 to I-68 |

Practising Law Institute
1177 Avenue of the Americas
New York, NY 10036
**#447969**