

Suggested Privacy and Cybersecurity Compliance Resources for U.S. Businesses

There are a number of publicly available resources to assist businesses in learning more about the legal and operational aspects of privacy and cybersecurity, and to help a business benchmark its program against industry practices. We list a few of those resources below, with a focus on toolkits and information sources available from government and non-profit websites and major industry participants. In addition to these resources, a business may wish to consult with its outside business partners for any free or low-cost resources that may be available. Such resources may include its commercial bank, its auditor, its insurance broker, its accountant or payroll processor, and its outside legal counsel. Larger businesses may also wish to reach out to their local federal law enforcement, such as the branch office of the FBI or Secret Service, to establish a relationship with them in the event that the business needs time-sensitive help in the future during a data security event.

Privacy

- **International Association of Privacy Professionals (IAPP).** The IAPP is the world's largest information privacy organization. Importantly, the IAPP is policy-neutral, in contrast to many other privacy organizations that advocate for a particular interest group. Serious privacy practitioners should consider joining the IAPP, although their website has free sources even for non-members on the general resources page, accessible at <https://iapp.org/resources/>. One particularly useful resource is the privacy legislation tracker: <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>. Another is the vendor marketplace: <https://iapp.org/resources/privacy-vendor-marketplace/>.
- **The Future of Privacy Forum (FPF).** FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices. FPF is independent, but not neutral, as it takes positions on particular pieces of proposed legislation and its scholarly articles are often action-directed. The blog (<https://fpf.org/blog/>) aggregates their white papers, reports, and other updates on regulation and legislation.
- **Microsoft's Compliance Center.** Many larger businesses run some version of Microsoft Office. Microsoft provides detailed guidance and instruction on how to use its existing product suites for particular compliance tasks, available here: <https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide>. This is an example of a resource that a business is often already paying for but that its privacy team may not yet know about, as it may be the domain of the business's IT department.
- **Service-specific privacy control centers.** Many businesses engage in digital advertising through online services, and those services have substantial rules, guidance, and controls that are accessible either publicly or through a log-in. Examples of these toolkits include Google Analytics (<https://support.google.com/analytics/answer/9019185?hl=en#zippy=%2Cin-this-article>) and Meta's marketing services for developers (<https://developers.facebook.com/docs/marketing-apis>). Similar to the Microsoft resource noted above, these resources may be the domain of a business's digital advertising team or website developers, but privacy professionals would be well served by understanding them as well.
- **OneTrust.** OneTrust is an industry leader in privacy program management, with a variety of solutions tailored to a specific law or regulation. Its blog is a good resource for updates and tips on privacy compliance, and is not too "salesy." The blog is accessible here: <https://www.onetrust.com/blog/>.
- **Federal Trade Commission (FTC).** The FTC has some helpful guidance on its Business Guidance Resources page, on a variety of privacy topics, including the Gramm-Leach-Bliley Act, accessible here: <https://www.ftc.gov/business-guidance/privacy-security>. The materials are not always timely, so a business should check the dates carefully.

Suggested Privacy and Cybersecurity Compliance Resources for U.S. Businesses

Cyber

- **InfraGard.** InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. critical infrastructure, including financial services. It is a great source of networking opportunities for cybersecurity professionals, and is organized around in-person meetings and a members-only website. It is organized in regional chapters, and there are sector-specific affinities, including active work for the financial services sector.
- **Cyber Fraud Task Forces (CFTFs).** This is the U.S. Secret Service's partnership organization with other law enforcement agencies, prosecutors, private industry, and academia. The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation. These are typically oriented around in-person events. Participation in a CFTF would be particularly meaningful for businesses interested in wire-diversion fraud, risks to payment card systems, and international funds transfers.
- **Cybersecurity & Infrastructure Security Agency (CISA).** CISA is a part of the U.S. Department of Homeland Security, and it is tasked with leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. It is not a law enforcement entity and was designed for collaboration and partnership. It has excellent free cybersecurity services and tools, available at <https://www.cisa.gov/free-cybersecurity-services-and-tools>.
- **US-CERT.** CISA houses US-CERT (Computer Emergency Readiness Team), which is responsible for analyzing and reducing cyber threats. US-CERT disseminates actionable cyber threat warnings to the private sector. The offerings also include self-assessment tools, at <https://www.cisa.gov/uscert/resources/assessments>.
- **StopRansomware.gov.** StopRansomware.gov is another CISA website dedicated to educating and assisting companies facing ransomware threats. It includes a cybersecurity evaluation tool at <https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr>.
- **Federal Communications Commission (FCC).** The FCC has some good online resources, including a customizable cyber security planning guide, available at <https://www.fcc.gov/cyberplanner>.
- **Small Business Administration (SBA).** The SBA has aggregated a list of free cybersecurity resources applicable to businesses of all sizes. They can be accessed here: <https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity>.

Contacts



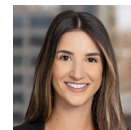
John E. Clabby
jclabby@carltonfields.com
www.carltonfields.com/jclabby
813.229.4229



Patricia M. Carreiro
pcarreiro@carltonfields.com
www.carltonfields.com/pcarreiro
305.539.7314



Joseph W. Swanson
jswanson@carltonfields.com
www.carltonfields.com/jswanson
813.229.4335



Eden Marcu
emarcu@carltonfields.com
www.carltonfields.com/emarcu
813.229.4148