

CIPP/US (Certified Information Privacy Professional US Private-Sector)

Course Description

SecureNinja's IAPP CIPP/US (2) two day training and certification boot camp in Washington DC, San Diego, CA and Live Online provides a foundational understanding of both broad global and concepts of privacy and data protection law and practice plus you have knowledge of these components within your concentration:

- Jurisdictional laws, regulations and enforcement models, or rules and standards
- Essential privacy concepts and principals
- Legal requirements for handling and transferring data

Originally launched in 2004 as the first professional certification ever offered in information privacy, the CIPP has become the preeminent credential in the field. It's also the IAPP's single largest educational program with several thousand certified professionals working in the field today (and earning more than they did before certification!)

The CIPP/US credential says you know privacy laws and regulations and how to apply them. It also says you know how to secure your place in the information economy.

Topics Covered

- Common principles and approaches to privacy
- Jurisdictions and industries
- Safeguarding personal information
- Online privacy
- US privacy environment
- Private-sector collection and data usage limitations
- Workplace privacy
- State privacy laws

What's Included

- Official IAPP CIPP participant guide
- Official IAPP CIPP textbook
- Official IAPP CIPP practice test
- IAPP CIPP/US certification exam voucher
- IAPP Membership for one year

Note: Your contact information must be provided to the IAPP and will be used by IAPP for membership services fulfillment in accordance with IAPP's policies.

Other Benefits

- Reduce risk of a data breach by making privacy a shared business objective
- Improve decision-making among employees who handle data

- Facilitate collaboration and communication across departments
- Demonstrate your commitment to data privacy and protection to customers, partners, regulators and staff

Who Should Attend

- Individuals who need a foundational understanding of information privacy and data protection
- Anyone interested in pursuing CIPP/US certification

Pre-requisites

There are no prerequisites

Exam Detail

IAPP CIPP/US

90 Questions 2.5 Hours

Course Length

2 days

Follow-on Courses

- CIPT (Certified Information Privacy Technologist)
- CIPM (Certified Information Privacy Manager)

Course Details

- I. Introduction to the U.S. Privacy Environment
 - A. Structure of U.S. Law
 - a. Branches of government
 - b. Sources of law
 - i. Constitutions
 - ii. Legislation
 - iii. Regulations and rules
 - iv. Case law
 - v. Common law
 - vi. Contract law

- c. Legal definitions
 - i. Jurisdiction
 - ii. Person
 - iii. Preemption
 - iv. Private right of action
- d. Regulatory authorities
 - i. Federal Trade Commission(FTC)
 - ii. Federal Communications Commission(FCC)
 - iii. Department of Commerce(DoC)
 - iv. Department of Health and Human Services(HHS)
 - v. Banking regulators
 - 1. Federal Reserve Board
 - 2. Comptroller of the Currency
 - vi. State attorneys general
 - vii. Self-regulatory programs and trustmarks
- e. Understanding laws
 - i. Scope and application
 - ii. Analyzing a law
 - iii. Determining jurisdiction
 - iv. Preemption
- B. Enforcement of U.S. Privacy and Security Laws
 - a. Criminal versus civil liability
 - b. General theories of legal liability
 - i. Contract
 - ii. Tort

- iii. Civil enforcement
 - c. Negligence
 - d. Unfair and deceptive trade practices(UDTP)
 - e. Federal enforcement actions
 - f. State enforcement (Attorneys General (AGs),etc.)
 - g. Cross-border enforcement issues (Global Privacy Enforcement Network(GPEN))
 - h. Self-regulatory enforcement (PCI, TrustMarks)
- C. Information Management from a U.S.Perspective
 - a. Data classification
 - b. Privacy program development
 - c. Incident response programs
 - d. Training
 - e. Accountability
 - f. Data retention and disposal (FACTA)
 - g. Vendor management
 - i. Vendor incidents
 - h. International data transfers
 - i. U.S. SafeHarbor
 - ii. Binding Corporate Rules(BCRs)
 - i. Other key considerations for U.S.-based global multinational companies
 - j. Resolving multinational compliance conflicts
 - i. EU data protection versus e-discovery
- II. Limits on Private-sector Collection and Use of Data
 - A. Cross-sector FTC Privacy Protection
 - a. The Federal Trade Commission Act

- b. FTC Privacy Enforcement Actions
- c. FTC Security Enforcement Actions
- d. The Children’s Online Privacy Protection Act of 1998(COPPA)
- B. Medical
 - a. The Health Insurance Portability and Accountability Act of 1996(HIPAA)
 - i. HIPAA privacy rule
 - ii. HIPAA security rule
 - b. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- C. Financial
 - a. The Fair Credit Reporting Act of 1970(FCRA)
 - b. The Fair and Accurate Credit Transactions Act of 2003(FACTA)
 - c. The Financial Services Modernization Act of 1999 (“Gramm-Leach-Bliley” orGLBA)
 - i. GLBA privacyrule
 - ii. GLBA safeguardsrule
 - d. Red Flags Rule
 - e. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
 - f. Consumer Financial Protection Bureau
- D. Education
 - a. Family Educational Rights and Privacy Act of 1974(FERPA)
- E. Telecommunications and Marketing
 - a. Telemarketing sales rule (TSR) and the Telephone Consumer Protection Act of 1991(TCPA)
 - i. The Do-Not-Call registry(DNC)
 - b. Combating the Assault of Non-solicited Pornography and Marketing Act of 2003(CAN-SPAM)
 - c. The Junk Fax Prevention Act of 2005(JFPA)

- d. The Wireless DomainRegistry
- e. Telecommunications Act of 1996 and Customer Proprietary Network Information
- f. Video Privacy Protection Act of 1988(VPPA)
- g. Cable Communications Privacy Act of1984
- III. Government and Court Access to Private-sector Information
- A. Law Enforcement and Privacy
 - a. Access to financial data
 - i. Right to Financial Privacy Act of1978
 - ii. The Bank Secrecy Act
 - b. Access tocommunications
 - i. Wiretaps
 - ii. Electronic Communications Privacy Act(ECPA)
 - 1. E-mails
 - 2. Stored records
 - 3. Pen registers
 - c. The Communications Assistance to Law Enforcement Act(CALEA)
- B. National Security and Privacy
 - a. Foreign Intelligence Surveillance Act of 1978(FISA)
 - i. Wiretaps
 - ii. E-mails and stored records
 - iii. National security letters
 - b. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-PatriotAct)
 - i. Other changes after USA-Patriot Act
- C. Civil Litigation and Privacy
 - a. Compelled disclosure of media information

- i. Privacy Protection Act of 1980
- b. Electronic discovery
- IV. Workplace Privacy
 - A. Introduction to Workplace Privacy
 - a. Workplace privacy concepts
 - i. Human resources management
 - b. U.S. agencies regulating workplace privacy issues
 - i. Federal Trade Commission(FTC)
 - ii. Department of Labor
 - iii. Equal Employment Opportunity Commission(EEOC)
 - iv. National Labor Relations Board(NLRB)
 - v. Occupational Safety and Health Act(OSHA)
 - vi. Securities and Exchange Commission(SEC)
 - c. U.S. Anti-discrimination laws
 - i. The Civil Rights Act of 1964
 - ii. Americans with Disabilities Act(ADA)
 - iii. Genetic Information Nondiscrimination Act(GINA)
 - B. Privacy before, during and after employment
 - a. Employee background screening
 - i. Requirements under FCRA
 - ii. Methods
 - 1. Personality and psychological evaluations
 - 2. Polygraph testing
 - 3. Drug and alcohol testing
 - 4. Social media

- b. Employee monitoring
 - i. Technologies
 - 1. Computer usage (including social media)
 - 2. Location-based services(LBS)
 - 3. Mobile computing
 - 4. E-mail
 - 5. Postal mail
 - 6. Photography
 - 7. Telephony
 - 8. Video
 - ii. Requirements under the Electronic Communications Privacy Act of 1986(ECPA)
 - iii. Unionized worker issues concerning monitoring in the U.S.workplace
- c. Investigation of employee misconduct
 - i. Data handling in misconduct investigations
 - ii. Use of third parties in investigations
 - iii. Documenting performance problems
 - iv. Balancing rights of multiple individuals in a single situation
- d. Termination of the employment relationship
 - i. Transition management
 - ii. Records retention
 - iii. References
- V. State Privacy Laws
 - A. Federal vs. state authority
 - B. Marketing laws
 - C. Financial Data

- a. Credit history
- b. California SB-1
- D. Data Security Laws
- a. SSN
- b. Data destruction
- E. Data Breach Notification Laws
 - a. Elements of state data breach notification laws
 - b. Key differences among states today

Go home certified!

About SecureNinja

SecureNinja Training is the DC's Area's #1 Expert IT Training Center . We are conveniently located in beautiful Historic Old Town Alexandria, VA enhancing your training experience and featuring:

- Metro Accessibility - Short walk from Metro Blue/Yellow Line (leave the car behind)
- 4 minute Drive to Ronald Reagan Washington National Airport
- Available Parking
- World class restaurants and shops at your footsteps
- Closest Expert IT & IT Security Training Center to Fort Belvoir, Boiling AFB, Fort Myer, Department of Homeland Security, US Department of Navy, US Coast Guard, Fort McNair, Washington Navy Yard

Why Choose SecureNinja for your Washington DC Expert IT Training?

- Expert Instructors
- Highest Pass Rates
- Choose from Day, Evening & Weekend Classes to meet your busy schedule
- Accelerated Boot Camps Save You Time And Money
- Paid Internships & Job Referrals!
- Meet Your DoD 8570-1 Certification Needs. Get Compliant!
- Secure Ninja is the ONLY Testing Center that offers ALL 5 industry standard test vendors in the DC / Baltimore Metropolitan Area. (VUE, Kryterion-Online, Certiport and Impact-Testing)
- Lowest Prices! We are locally based keeping our overhead low so we can pass the savings along to you
- Washington, DC is our Home. Most training centers set up shop in hotels or rented centers. When you have a need, request or encounter a problem they are not there to answer. Our physical location in Alexandria is open 7 days a week and our staff always there to help.