U.S. GOVERNMENT PRIVACY

This training is a robust, interactive opportunity to learn about critical privacy concepts that are also integral to the CIPP/G exam. While not purely a "test prep" course, this training is appropriate for professionals who plan to certify, as well for those who want to deepen their privacy knowledge. Both the training and the exam are based on the same body of knowledge.

LIVE TRAINING

MODULES

Module 1: Privacy Definitions and Principles
Introduces definitions of privacy and PII, explains the importance of privacy as a core value in U.S. society, reviews the FIPPs, and compares and contrasts information privacy and information security.

Module 2: OMB Circular A-130 Core Concepts
Explains the purpose of the Federal Privacy Council, describes the duties of the SAOP, reviews general requirements of agency privacy programs, summarizes the concepts and practice of continuous monitoring and describes agency responsibilities for employee and contractor training and accountability.

Module 3: The Privacy Act of 1974
Reviews the major purpose and policy objectives of the Privacy Act of 1974, to whom it applies and whom it protects, as well as which agencies are exempt from specific provisions of the Act; describes the intention of systems of records and systems of records notices; summarizes the benefits of computer matching programs and the privacy protections built into them; reviews the civil remedies and criminal penalties for Privacy Act violations.

Module 4: The E-Government Act of 2002
Reviews the purpose and policy objectives of the E-Government Act of 2002; provides the definition of a PIA, describes when to conduct one and, at a high level, what information needs to be included; describes website privacy policy requirements and content for agency-facing public websites; outlines appropriate agency uses for, and how to communicate privacy protections when working with, third-party websites and applications (TPWA).

Module 5: Other U.S. Government Privacy Laws
Explains the implications of the Federal Information Security Management Act (FISMA) for federal agencies; describes key responsibilities of federal agencies as a result of several U.S. government privacy laws, including: the Paperwork Reduction Act, Data Quality Act, Federal Agency Data Mining Reporting Act, Federal Records Act, Controlled Unclassified Information (CUI) Office Notice, and Cybersecurity Information Sharing Act (CISA); describes the objective of federal open meetings laws.

Module 6: Risk Management and Incident Response
Reviews the various NIST publications and OMB memoranda that govern risk management of privacy and security in government systems, as well as the Fair Information Practice Principles (FIPPs) underlying these standards; describes agency requirements for tracking and documenting breach response activities, according to OMB M-17-12; explains the difference between incidents and breaches; introduces the three privacy engineering objectives outlined in NISTIR 8062, "An Introduction to Privacy Engineering and Risk Management in Federal Systems."

Module 7: Other U.S. Government Privacy Practices
Describes the rights granted by the Freedom of Information Act (FOIA) of 1966, as well as several exceptions to the act and the purpose of institutional review boards (IRBs); reviews the privacy-related requirements set forth by OMB M-17-06, "Policies for Federal Agency Public Websites and Digital Services."; explains privacy safeguards that agencies should put into place when working with contractors and third parties.

Module 8: Laws Affecting Both the Public and Private Sectors
Identifies the privacy-related components of laws related to protected health information (PHI); describes the major points of laws relating to intelligence and homeland security; explains the significant differences, from a privacy perspective, between the USA PATRIOT Act and the USA FREEDOM Act, reviews federal government aspects of privacy-related laws in the financial and communications sectors.

Module 9: U.S. Constitutional Issues
Describes the Fourth Amendment and the related questions used to evaluate whether an individual's rights under this amendment have been violated; reviews the concept of third-party doctrine; reviews the Stored Communications Act.

Module 10: Guidance and Reporting Summary
Summarizes the primary privacy reporting obligations of federal agencies; refers to a full list of memoranda, law, directives, executive orders and other guidance covered in the training.