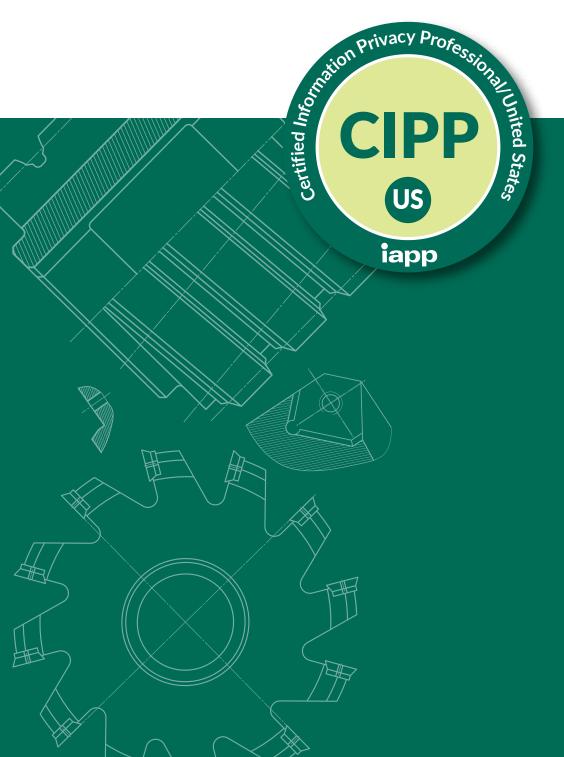
## CERTIFICATION EXAMINATION BLUEPRINT





**Controlled Document** 

Page 1 of 2

Approved by: EDB/CIPPUS

Effective Date: 10/02/23

international association of privacy professionals

Version 2.4.2 Approved on: 3/8/2023

**Supersedes: 2.4.1** 

## U.S. Private-sector Privacy Certification

Examination Blueprint for the Certified Information Privacy Professional/United States (CIPP/US™)



The examination blueprint indicates the minimum and maximum number of question items that are included on the CIPP/US examination from the major areas of the Body of Knowledge. Questions may be asked from any of the listed topics under each area. You can use this blueprint to guide your preparation for the CIPP/US examination.

I. In	troduction to the U.S. Privacy Environment	27	35
A.	Structure of U.S. Law Branches of government, sources of law, legal definitions, regulatory authorities, understanding laws	4	6
В.	Enforcement of U.S. Privacy and Security Laws Criminal vs. civil liability, general theories of legal liability	5	7
C.	Information Management from a U.S. Perspective Data inventory and classification, data flow mapping, privacy program development, managing user preferences, incident response programs, workforce training, accountability, data and records retention and disposal (FACTA), online privacy, privacy notices, vendor management, international data transfers and Schrems decisions, other key considerations for U.Sbased multinational companies (including GDPR requirements, APEC), resolving multinational compliance conflicts	18	22
II. Li	mits on Private-sector Collection and Use of Data	15	25
Α.	Cross-sector FTC Privacy Protection The FTC Act, FTC privacy enforcement actions, FTC security enforcement actions, COPPA, future of federal enforcement	5	7
В.	Healthcare/Medical HIPAA, HITECH, GINA, The 21 <sup>st</sup> Century Cures Act of 2016, Confidentiality of Substance Use Disorder Patient Records Rule	4	6
C.	Financial	4	6

Controlled Document Approved by: EDB/CIPPUS Effective Date: 10/02/23

Page 2 of 2

Version 2.4.2 Approved on: 3/8/2023 Supersedes: 2.4.1



	FCRA, FACTA, GLBA, Red Flags Rules, Dodd-Frank, CFPB, online banking		
D.	Education	1	3
	FERPA, education technology		
E.	Telecommunications and Marketing	1	3
		_	•
III.	<b>Government and Court Access to Private-sector Information</b>	3	7
Α.	Law Enforcement and Privacy	1	3
	Access to financial data, access to communications, CALEA		
В.	National Security and Privacy	1	2
	FISA, USA-Patriot Act, USA Freedom Act, Cybersecurity Information Sharing Act		
	(CISA)		
C.	Civil Litigation and Privacy	1	2
	Compelled disclosure of media information, electronic discovery		
IV.	Workplace Privacy	5	9
A.	Introduction to workplace privacy	2	4
	Workplace privacy concepts, U.S. agencies regulating workplace privacy issues,		
	U.S. anti-discrimination laws		
В.	Privacy before, during and after employment	3	5
	Automated employment decision tools and potential for bias, employee		
	background screening, employee monitoring, investigation of employee		
	misconduct, termination of employment relationship, working with third parties		
V. St	ate Privacy Laws	9	15
Α.	Federal vs. state authority	1	3
В.	Data privacy and security laws	6	8
C.	Data breach notification laws	2	4