CSBA GROUP
Cyber Security Board Advisors

Cyber Security Regulations Guide

Regulatory Identifier	Regulatory Description & Enforcement	Requirements	Penalties
CFTC FINANCE Commodity Futures Trading Commission ❖ CFR TITLE 17 PART 39B ❖ FINRA DETAILS	The CFTC regulates Derivatives Clearing Organizations. These organizations are purposed to clear transactions for commodities trading of futures and options. CFTC regulations are enforced by the Securities & Exchange Commission (SEC) and by the nonprofit entity Financial Industry Regulatory Authority (FINRA).	❑ Compliance report sent to the Board & CFTC ❑ Vulnerability testing of contractors 2x/quarter ❑ Annual internal/external penetration test ❑ Control testing once every three years ❑ Annual security incident response plan testing	Up to $1M or 3x the monetary gain per infraction
COPPA ALL SECTORS Children's Online Privacy Protections Act ❖ US CODE 15 CHAPTER 91 ❖ CFR TITLE 16 PART 312	Applies to websites and online services which knowingly, or are purposed to, collect personal information of children under 13 years of age; regulates how sites collect, use, or disclose information about children. The Act is enforced by the Federal Trade Commission (FTC).	❑ Obtain parental consent before any collection ❑ Provide reasonable means to review the data ❑ Cannot require participation to share data ❑ Must have a security program to protect data ❑ Must provide privacy notice; how data is used	Up to $40K per record
DFAR DoD & CONTRACTORS Defense Federal Acquisition Regulation ❖ CFR TITLE 48 PART 252.204 ❖ DFAR 239.71	DFAR applies to all US Government (USG) Department of Defense (DoD) entities and contractors who process, store, or transmit covered defense information; more than just alignment to security best practice; DFAR requires adherence to multiple regulatory standards including NIST, FIPS, and DoD Instructions.	❑ Compliance with NIST 800-171 ❑ Compliance with the Clinger-Cohen Act ❑ Compliance with FIPS for impact and processing ❑ Compliance with DoD Directives 8140 & 8500 ❑ Immediately report all cyber incidents to DoD	Loss of license and disbarment
ECPA ALL SECTORS Electronic Communications Privacy Act ❖ US CODE 18 CHAPTER 119 ❖ US CODE 18 CHAPTER 121	The ECPA protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. The Act is enforce by the Department of Justice (DoJ).	❑ Implement policy to prohibit recording or disclosing any communications without consent ❑ Implement policy to prohibit surveillance of non-employees without consent; allowable for employees with valid business reason	Criminal penalties & civil punitive damages
FDA PHARMA & HEALTH CARE Food and Drug Administration ❖ CFR TITLE 21 PART 11 ❖ FDA CYBER GUIDANCE	The FDA regulates the use of electronic records within clinical investigations; they also provide cyber security guidance for medical device manufacturers. The current regulations apply to organizations involved in clinical investigations of medical products, including sponsors, clinical investigators, review boards, and contract research organizations.	❑ Must limit system access to authorized individuals ❑ Ensure system reliability ❑ Maintain system audit trail ❑ Implement policies which govern user accountability	Varies based on violation; ranges between $10K - $1M
FERPA EDUCATION Family Educational Rights and Privacy Act ❖ CFR TITLE 34 PART 99 ❖ DEPT OF EDUCATION	The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. The law applies to all schools that receive funds under the U.S. Department of Education and prohibits institutions from disclosing "personally identifiable education information" such as grades or financial aid information without the student's permission.	❑ Student information must be protected in a manner that does not permit personal identification of individuals by anyone other than the officials or authorized agencies ❑ Required data breach notification to DoE	Criminal & civil punitive damages [6 months +$1K]

Cyber Security Regulations Guide

Regulatory Identifier	Regulatory Description & Enforcement	Requirements	Penalties
FISMA ALL FEDERAL AGENCIES Federal Information Security Management Act ❖ US CODE 44 CHAPTER 35 ❖ NIST CSRC RISK MGMT.	FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security respective operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. There is also an amended 2014 version to 'Modernize' certain areas of the regulation. DHS enforced.	❑ Keep system & data inventory and risk categorized ❑ Define and maintain a system security plan ❑ Periodically review system security controls ❑ Conduct annual security reviews to ensure FISMA compliance	Censure by Congress, reduction of funding, reputational damage
FTC ALL SECTORS Federal Trade Commission ❖ US CODE 15 CHAPTER 2 ❖ CFR TITLE 16 PART 314	The FTC has jurisdiction over all entities, with exception to banks and common carriers (both having prescriptive regulations within their own sector). Justification for its oversight is rooted in a 1914 law prohibiting deceptive practices (section 5 of FTC Act) and its Safeguard regulations 16 CFR 314 enforced through the Gramm-Leach-Bliley Act (GLBA).	❑ Must engage in "reasonable and necessary" security practices; generally undefined ❑ Insure the security and confidentiality of customer information; protect against unauthorized access ❑ Protect against any anticipated threats or hazards to the security or integrity of such information	Undefined but common penalties ~ $10K range with instances in $M
GDPR ALL SECTORS WITH EU CUSTOMERS General Data Protection Regulation ❖ REGULATION 2016/679 ❖ GDPR KEY CONCEPTS	GDPR regulates privacy data of EU residents, whether the information was obtained through an EU-based entity or not. It was enacted in 2018 and required compliance by May 25th in the same year. The GDPR enforcement body, IAPP, has already begun taking enforcement actions, largely targeting marketing, criminal justice, health, and financial services entities.	❑ Entities must have a Data Protection Officer (DPO) ❑ Consumer Privacy Data must be protected ❑ Entities must maintain a process for users to request knowledge of their data ❑ User Data Rights; right to Access, Rectification, Erasure, and Data Portability	4% of annual global turnover or €20M – whichever is greater
GLBA FINANCIAL SECTOR Gramm-Leach-Bliley Act ❖ CFR TITLE 16 PART 314 ❖ US CODE 15 CHAPTER 94	GLBA is both and information security and a privacy law applicable to financial institutions (a broad definition that includes entities like banks, insurance companies, securities firms, non-bank mortgage lenders, auto dealers, and tax preparers). Enforcement entity depends on the type of financial institution being regulated; often performed by FDIC.	❑ Implement and maintain a comprehensive data security program; includes Board of Directors ❑ Apply risk management and assessment practices ❑ Implement an incident response plan and training ❑ Maintain oversight of supplier risks	Up to $1M and termination of FDIC insurance
HIPAA HEALTH CARE Health Insurance Portability and Accountability Act ❖ CFR TITLE 45 PART 160 ❖ CFR TITLE 45 PART 164	HIPAA regulations apply to any company that deals with healthcare data, such as healthcare providers and plan administrators (including doctor's offices and insurance companies). General employers are not under HIPAA enforcement, but their employee data (PHI) must be handled accordingly. The Act is enforced by Health & Human Services Office for Civil Rights.	❑ The confidentiality, integrity, and availability of electronic health information (ePHI) be protected ❑ Individuals be notified within 60 days of a breach ❑ Breaches >500 persons require notice to the media and the Secretary of Health and Human Services	Varies based on violation; largest penalty exceeds $5M
PCI CREDIT CARD HANDLING Payment Card Industry ❖ PCI-DSS VERSION 3.2 ❖ PCI SECURITY STANDARDS COUNCIL	Payment Card Industry's Data Security Standards (PCI-DSS) apply to entities handling credit card data. PCI is most interested in card issuers, points of sale merchants, and acquiring banks, but any entity processing, storing, or transmitting card holder data is in scope. Compliance requirements vary depending on the quantity of transactions made.	❑ Build and maintain a secure network ❑ Protect cardholder data ❑ Maintain vulnerability management program ❑ Implement strong access control measures ❑ Regularly monitor and test networks ❑ Maintain an Information Security policy	$5K-$100K per month penalties; issued to acquiring bank and passed to merchant

Cyber Security Regulations Guide

Regulatory Identifier	Regulatory Description & Enforcement	Requirements	Penalties
SEC FINANCE Securities and Exchange Commission ❖ CFR TITLE 17 PART 248A ❖ CFR TITLE 17 PART 248C	SEC Rule 30 applies to US and foreign brokers, dealers, investment companies, and investment advisers that are registered with the SEC. Enforcement carried out by SEC, or FINRA, but companies may also be subject to the concurrent jurisdiction of the New York Department of Financial Services (NYDFS) cybersecurity regulations (23 NYCRR 500) .	❑ Adopt policies and procedures to protect customer data from cyber-attacks & unauthorized access ❑ Provide initial and annual privacy notices to customers describing information sharing policies ❑ Secure disposal of information to protect against unauthorized access	Up to $1M or 3x the monetary gain per infraction
SOX ALL PUBLIC COMPANIES Sarbanes-Oxley Act ❖ US CODE 15 CHAPTER 98 ❖ SARBANES-OXLEY ACT 2002	SOX is purposed to make sure public companies produce accurate financial statements; thus the cyber security requirements are aimed at protecting access and integrity of data. Recent updates to Sections 302 & 404 provide more security guidance. SOX is enforced by the Security & Exchanges Commission and extend to criminal penalties reaching C-level liability.	❑ Maintains processes and standards for applying internal controls across 5 defined domains: Control Environment. Risk Assessment, Control Activities, Information and Communication, and Monitoring ❑ Incident response and reporting requirements	Criminal & civil punitive damages up to 20 yrs + $5M
STATE ENTITY W/BUSINESS IN STATE There are multiple state regulations (i.e. CCPA) ❖ BREACH LAWS (ALL STATES) ❖ PRIVATE SECTOR (ALL STATES)	24 of the US states have Data Security Laws for the Private Sector. All states have breach notification laws. California is leading the data privacy regulations effort through their California Consumer Protection Privacy Act. Common among these current and emerging regulations is the need to protect privacy data, notify of breach, and dispose when asked.	❑ Requirements vary by state; but common practices include: implementing adequate security controls and practices to protect the confidentiality of consumer data ❑ All states have breach notification requirements which outline timeframe and penalties	Vary by state

ABOUT THIS GUIDE

- ❑ The Guide is focused on the most common regulations impacting US-based companies in the areas of cyber security and data privacy
- ❑ The Requirements section is intended to focus on the unique attributes of each regulation respectively; though not continually stated, nearly every one of these regulations requires the applicable company to maintain a best practice Information Security & Data Privacy program
- ❑ The Penalties section identifies the range or maximum allowable retribution for non compliance to the respective regulations
- ❑ Make sure to check out the reference links listed under each regulatory identifier; most of the content provided for this guide comes directly from federal and industry sources
- ❑ While the Guide includes various regulatory entities across many industry sectors, there are still more less-known local, federal, and industrial regulations not included; this Guide should be used only to jumpstart your compliance efforts, not relied upon for complete assurance of your regulatory requirements