ACTIVATION CAPITAL
From start to phenomenal

GENEDGE

Cybersecurity Frameworks Summary

	National Institute of Standards and Technology (NIST) Cybersecurity Framework (CFS)	National Institute of Standards and Technology (NIST) 800-53	National Institute of Standards and Technology (NIST) 800-171	National Institute of Standards and Technology (NIST) 800-171 Cybersecurity Maturity Model Certification (CMMC) Level 1	National Institute of Standards and Technology (NIST) 800-171 Cybersecurity Maturity Model Certification (CMMC) Level 2	Health Industry Cybersecurity Practices (HICP)	Healthcare and Public Health Sector Specific Cybersecurity Performance Goals (CPGs)	International Traffic in Arms Regulations (ITAR)	Health Insurance Portability and Accountability Act (HIPAA) Security Rule
Link	https://www.nist.gov/cyberframework	SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)	https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final	https://dodcio.defense.gov/CMMC/About/	https://dodcio.defense.gov/CMMC/About/	https://405d.hhs.gov/cornerstone	https://hphcyber.hhs.gov/performance-goals.html	https://www.federalregister.gov/documents/2023/02/27/2023-03828/international-traffic-in-arms-regulations-consolidation-and-restructuring-of-purposes-and	https://www.hhs.gov/hipaa/for-professionals/security/index.html
Description	The NIST Cybersecurity Framework provides a comprehensive set of guidelines and best practices designed to help organizations manage and reduce cybersecurity risks.	NIST Special Publication 800-53 offers a catalog of security and privacy controls for federal information systems and organizations to protect against cyber threats and enhance information security.	NIST Special Publication 800-171 provides guidelines for protecting Controlled Unclassified Information (CUI) in non-federal information systems and organizations.	The Cybersecurity Maturity Model Certification (CMMC) Level 1 represents the foundational tier, requiring organizations to implement basic cyber hygiene practices.	CMMC Level 2 acts as an intermediate stage, requiring organizations to document and implement specific cybersecurity practices to protect Controlled Unclassified Information (CUI) and prepare for more advanced cybersecurity measures.	The HICP provides tailored cybersecurity guidelines designed to help healthcare organizations of all sizes mitigate threats and protect patient information.	The Healthcare and Public Health Sector-Specific CPGs offer a set of cybersecurity benchmarks and objectives tailored to address the unique threats and vulnerabilities faced by the healthcare and public health sector.	ITAR cybersecurity requirements mandate the protection and control of technical data related to defense articles and services, ensuring it is not accessed or transferred to unauthorized non-U.S. persons without proper authorization.	The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information by requiring appropriate administrative, physical, and technical safeguards.
Issuing Agency	U.S. Department of Commerce National Institute of Standards and Technology (NIST)	U.S. Department of Commerce National Institute of Standards and Technology (NIST)	U.S. Department of Commerce National Institute of Standards and Technology (NIST)	U.S. Department of Defense (DoD) U.S. Department of Commerce National Institute of Standards and Technology (NIST)	U.S. Department of Defense (DoD) U.S. Department of Commerce National Institute of Standards and Technology (NIST)	U.S. Department of Health and Human Services (HHS) in coordination with Health Sector Coordinating Council (HSCC)	U.S. Department of Health and Human Services (HHS) U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)	U.S. Department of State Directorate of Defense Trade Controls (DDTC)	U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)
Current Version (as of March 2024)	February 2024 Version 2.0	September 2020 Revision 5	February 2020 Revision 2	November 2021 CMMC 2.0	November 2021 CMMC 2.0	April 2023 2023 Edition	January 2024 First Release	February 2023 Final Rule	January 2013 NIST SP800-66 Rev 2 HIPAA Security Rule Guidanace Released in Feb 2024.
Requirements Framework Organization	5 Core Functions 23 Categories 108 Subcategories / Practices	20 Control Families 1000+ controls	14 Control Families 110 Controls	5 Control Families 17 Controls	14 Control Families 110 Controls	10 Practices 43 Sub Practices (Vol 1.Small Business) 88 Sub Practices (Vol 2. Medium Business)	20 Goals: 10 Essential Goals 10 Enhanced Goals	ITAR itself does not detail specific cybersecurity practices (like encryption standards or specific technical measures), it mandates a general requirement to protect controlled technical data from unauthorized access.	3 Safeguards 18 Standards 37 Implementation Specifications
Target Users	Organizations of all sizes and sectors, including private sector companies, government agencies, and critical infrastructure providers.	Federal agencies and organizations, as well as contractors and other entities that work with federal information systems.	Non-federal organizations, including contractors and subcontractors, that handle, process, store, or transmit Controlled Unclassified Information (CUI) on behalf of the federal government.	Contractors and subcontractors within the Defense Industrial Base (DIB) that handle Federal Contract Information (FCI) but not Controlled Unclassified Information (CUI), requiring basic cybersecurity hygiene practices to protect that information.	Contractors and subcontractors within the Defense Industrial Base (DIB) that handle Controlled Unclassified Information (CUI) and need to implement intermediate cybersecurity practices to protect this information, serving as a transition to more advanced cybersecurity measures.	Healthcare organizations of all sizes, including small, medium, and large providers, aiming to enhance their cybersecurity measures and protect patient information.	Organizations and entities within the healthcare and public health sector, including hospitals, clinics, care providers, public health departments, and other healthcare services, aiming to enhance their cybersecurity posture.	U.S. and foreign entities engaged in the manufacturing, export, brokering, or transferring of defense articles, services, and related technical data listed on the United States Munitions List (USML).	Covered entities (such as healthcare providers, health plans, and healthcare clearinghouses) and their business associates who handle electronic protected health information (ePHI).