Nist Standards for Research Reference

* NIST Special Publication (SP) 800-128: Guide for Security-Focused Configuration and Management of Information Systems
  + This goes over establishing secure baselines, continuous monitoring, and integrating security into configuration management.
* NIST Interagency Report (IR) 8425A: Recommended Cybersecurity Requirements for Consumer-Grade Router Products
  + This outlines security features and practices that manufacturers should implement
  + Use this for baseline.
    - Asset Identification – require SSIDs, component inventory of all connected components.
    - Configuration – Config should be restricted access, strong authentication mechanisms, MFA, Factory reset ability
    - Encryption – data stored in routers such as credentials must use strong encryption methods in line with FIPS 140-3
    - Data in transit – Must be encrypted
    - Interface Access – unnecessary interfaces should be disabled by default or removed. Strong access control only allow authorized people to interact with routers functionality.
    - Timely Notifications – entities should be notified if a security event is triggered within the router.
* NIST Cybersecurity for IoT Program: Consumer IoT Cybersecurity
  + This mainly focuses on IoT but includes consumer-grade routers and provides guidelines for security and resources.
  + Overlaps with 8425A

IETF

* IETF RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
  + Provides the framework for networking device profiles for ISP’s to communicate their security requirements with equipment vendors.
  + Guidelines on secure configuration, access controls, and security assessments.

ISO

* ISO/IEC 27001:2022 – Information Security Management Systems
  + Security controls that can be applied to routers and risk management.