**Build and Operate a Trusted DoIN**

**Cybersecurity-Related Policies and Issuances**
- Developed by the DoD Deputy CIO for Cybersecurity
- Last Update: February 1, 2021
- Send questions/suggestions to info@caloc.org

**National/Federal**
- **NIST**
  - Special Publication 800 Series
    - NIST SP 800-53, Security and Privacy Controls for Federal Information Systems
    - NIST SP 800-77, Recommendations for Wired and Wireless Information Technology Security Controls
    - NIST SP 800-82, Guide for Implementing Intrusion Detection and Prevention Systems
    - NIST SP 800-160, Directing the Priority Research and Development of Information Technology Provisions
    - NIST SP 800-208, Use of Path Validation Technology in Cloud Computing, Internet of Things (IoT), and Other Industrial Control Systems
    - NIST SP 800-213, Guide for Implementing Risk Management for Cybersecurity
    - NIST SP 800-38B, Guidelines for Implementing Cryptographic Key Management
    - NIST SP 800-50, Guide for Conducting Risk Assessments

**Operational**
- **NIST**
  - Special Publication 800 Series
    - NIST SP 800-53, Security and Privacy Controls for Federal Information Systems
    - NIST SP 800-77, Recommendations for Wired and Wireless Information Technology Security Controls
    - NIST SP 800-82, Guide for Implementing Intrusion Detection and Prevention Systems
    - NIST SP 800-160, Directing the Priority Research and Development of Information Technology Provisions
    - NIST SP 800-208, Use of Path Validation Technology in Cloud Computing, Internet of Things (IoT), and Other Industrial Control Systems
    - NIST SP 800-213, Guide for Implementing Risk Management for Cybersecurity
    - NIST SP 800-38B, Guidelines for Implementing Cryptographic Key Management
    - NIST SP 800-50, Guide for Conducting Risk Assessments

**Subordinate Policy**
- **NIST**
  - Special Publication 800 Series
    - NIST SP 800-53, Security and Privacy Controls for Federal Information Systems
    - NIST SP 800-77, Recommendations for Wired and Wireless Information Technology Security Controls
    - NIST SP 800-82, Guide for Implementing Intrusion Detection and Prevention Systems
    - NIST SP 800-160, Directing the Priority Research and Development of Information Technology Provisions
    - NIST SP 800-208, Use of Path Validation Technology in Cloud Computing, Internet of Things (IoT), and Other Industrial Control Systems
    - NIST SP 800-213, Guide for Implementing Risk Management for Cybersecurity
    - NIST SP 800-38B, Guidelines for Implementing Cryptographic Key Management
    - NIST SP 800-50, Guide for Conducting Risk Assessments

**About This Chart**
- This chart organizes cybersecurity policies and guidelines by strategic policy office or primary responsibility (see Color Key). Double-clicking on the box directs users to the most authoritative publicly accessible resource.
- Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hypertext is currently available.
- The linked sites are not controlled by the developers of this chart. We checked the sites to ensure the links are on a regular basis, but you may occasionally experience an error message due to problems at the source site or a policy decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSN policies link only to the CNSN site, per restrictions implemented by...