CYBERSECURITY HIGHLIGHTS[1]

Enclosed are the links to a subset of cybersecurity formal publications that are of interest to a wide audience. Please ensure that TLS 1.2 is active in your browser. Consult reputable sources for information on how to set and verify that TLS 1.2 is active for your particular browser.

NETWORK MITIGATIONS PACKAGE

- Network Mitigation Package- Infrastructure
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/network-mitigations-package-infrastructure.cfm
- Segregate Network and Functions
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/segregate-networks-and-functions.cfm
- Limit Workstation to Workstation Communication
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/limit-workstation-to-workstation-communication.cfm
- Harden Network Devices
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/harden-network-devices.cfm
- Secure Access to Infrastructure Devices
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/secure-access-to-infrastructure-devices.cfm
- Perform Out-of-band Network Management
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/perform-out-of-band-network-management.cfm
- Validate Integrity of Hardware and Software
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/validate-integrity-of-hardware-and-software.cfm

[1] The information contained in this document was developed in the course of NSA's cybersecurity mission including its responsibilities to identify and disseminate information on threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-related products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

HOST/NETWORK/CLOUD SECURITY AND IDENTITY THEFT PROTECTION

- Manageable Network Plan
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/manageable-networkplan.cfm

- Host Mitigation Package
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/host-mitigation-package.cfm

- Cloud Security Considerations
  https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/cloud-security-considerations.cfm

- Best Practices for Keeping Your Home Network Secure
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf

- Identity Theft Threat and Mitigations
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-indentity-theft-threat-and-mitigations.pdf

TOP 10 CYBERSECURITY MITIGATION STRATEGIES 2018

More documents are in progress for this category and will be published when available.

- NSA's Top 10 Cybersecurity Mitigation Strategies
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

- UEFI Advantages Over Legacy Mode
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-uefi-advantages-over-legacy-mode.pdf

- UEFI Lockdown Quick Guidance
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-uefi-lockdown.pdf

ENDPOINT AND OTHER CYBERSECURITY MITIGATION STRATEGIES

- Take Advantage of Software Improvements
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/take-advantage-of-software-improvement.cfm
- Windows 10 for Enterprises Security Benefits of Timely Adoption
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-windows-10-for-enterprise-security-benefits-of-timely-adoption.pdf
- Application Whitelisting
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/application-whitelisting.cfm
- Control Administrative Privileges
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/control-administrative-privileges.cfm
- Limit Workstation to Workstation Communication
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/limit-workstation-to-workstation-communication.cfm
- Anti-virus Reputation Services
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/anti-virus-reputation-services.cfm
- Anti-exploitation Features
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/anti-exploitation-features.cfm
- Host Intrusion Prevention Systems
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/host-intrusion-prevention-systems.cfm
- Secure Host Baseline
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/secure-host-baseline.cfm
- Blocking Unnecessary Advertising Web Content
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-blocking-unnecessary-advertising-web-content.pdf
- Web Domain Name System Reputation
  https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/web-domain-name-system-reputation.cfm
- Steps to Secure Web Browsing
  https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-steps-to-secure-web-browsing.pdf

Disclaimer of Warranties and Endorsement
The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information
Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov