



INFORMATIONAL

NSA Releases Network Infrastructure Security Guidance for Network Administrators



TLP:WHITE

Mar 03, 2022

The United States National Security Agency (NSA) has released a new [Cybersecurity Technical Report \(CTR\): Network Infrastructure Security Guidance](#). The report captures several best practices based on the depth and breadth of experience in supporting organizations and responding to threats. Network environments are dynamic and evolve as new technologies, exploits, and defenses affect them. While compromise occurs and is a risk to all networks, network administrators can greatly reduce the risk of incidents as well as reduce the potential impact in the event of a compromise. This guidance featured here in this alert focuses on the design and configurations that protect against common vulnerabilities and weaknesses on existing, targeted networks.

The report classified the best practices into several areas, including network architecture and design, security maintenance, authentication, authorization, accounting, remote logging and

monitoring, administrator accounts, and passwords. Recommendations include perimeter and internal network defenses to improve monitoring and access controls throughout the network. When it comes to security maintenance, NSA calls on organizations to verify software and configuration integrity, maintain updated operating systems and software, stay current with vendor-backed hardware and maintain proper file system and boot management.

Health-ISAC is sharing this CTR for your internal security awareness and as a compendium for network best practices within your technological environment. The full report, which is attached to this alert in Health-ISAC Threat Intelligence Portal (HTIP) for your convenience, can also be accessed [here](#).

Reference(s)

[executivegov](#), [Defense](#)

Release Date

Mar 03, 2022

Alert ID d36c9b0d

[View Alert](#)

Tags Network Infrastructure, NSA Advisory, Network Infrastructure Devices, NSA, Networks, Administrators, network

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. |



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.

Powered by [Cyware](#)