# INFORMATION ASSURANCE DIRECTORATE

**"INFORMATION ASSURANCE LEADERSHIP FOR THE NATION"**

**(U) INFORMATION ASSURANCE** **Date: 29 April 2013**
**(U) ADVISORY NO. IAA-005-2013**

**SUBJECT**: (U) Hardening Network Infrastructure: Security Recommendations for System Accreditors

1. (U) **Purpose:** Many networks run by public and private organizations have experienced intrusions in recent years, and this cyber exploitation has resulted in an unprecedented transfer of wealth due to lost intellectual property. The threats to our networks and systems exist across numerous components that include end-user-devices, servers, and infrastructure devices. To address threats to routers and other network infrastructure devices, the National Security Agency's Information Assurance Directorate (IAD) is publishing this IAA to guide U.S. Government systems accreditors' strategic plan for network hardening. IAD will also be releasing an UNCLASSIFIED Factsheet (MIT-003FS-2013) with the same recommendations to help other public and private sector organizations combat the challenge of cyber exploitation through hardening networks.

2. (U) **Security Recommendations**

(U) Device Integrity

- Purchase network hardware only from the manufacturer or from resellers who are authorized and certified by the equipment manufacturer.
- Use a trusted administrative workstation to compare the file hash for network device firmware to the manufacturer's published hash before installing new firmware on a network device. Periodically re-verify the file hash of the running firmware while the network device is in operation.
- Avoid installing and do not run network device firmware versions that are no longer available from the manufacturer.
- Shut down unused physical interfaces on network devices.
- Implement access lists that allow only those protocols, ports and IP addresses that are required by network users and services, and then deny everything else.
- Protect the network device configuration file from unauthorized disclosure. Take steps to avoid the appearance of plaintext passwords in the configuration file. Using encryption and/or a salted hash with iteration is critical to protect the confidentiality of passwords in configuration files—encoding alone is not enough.

- Change passwords/keys immediately if the network device configuration file is transmitted in the clear (or is otherwise exposed) while containing non-encrypted passwords/keys.
- Use secure protocols when transmitting network device configuration files.
- Ensure that an audit event is created upon reboot and when configuration changes are applied to network devices.
- Shut down unneeded services on network devices.
- Review logs periodically to gain an in depth understanding of normal network behavior.

(U) Secure Management

- Only use secure protocol standards (SSHv2; IKEv2/IPsec; TLS v1.0+) when performing remote management of network devices. For further details, see Annex C of NIAP's Network Device Protection Profile (NDPP) – http://www.niap-ccevs.org/pp.
- Restrict remote management connectivity to only controlled machines that are on a separate security domain with robust protection.
- Create and maintain a written network infrastructure security policy. This policy should identify who is allowed to log in to network infrastructure devices and who is allowed to configure network devices, and should define a plan for updating network device firmware at scheduled intervals.
- Never use default usernames and/or passwords. The network infrastructure security policy should define password length and complexity requirements.
- Use at least two authenticated NTP sources to maintain a consistent time among network devices.

(U) Secure Protocol Standards + Strong Cryptography

- Follow NIST SP 800-131A guidance for cryptographic algorithm and key lengths when performing remote management of network devices, (e.g., transition to 2048-bit DH modulus for SSH key agreement and 2048-bit RSA certificates for SSH authentication).
- When using SNMP, use SNMPv3 with encryption enabled and/or encapsulate all SNMP traffic in an IPsec tunnel.
- All IPsec VPNs should conform to IETF standards and NIST SP 800-131A guidance. Employ IETF secure protocol standards where possible.
- Invoke the FIPS 140 evaluated crypto engine in the network device, and configure algorithm selections that were validated through an NDPP evaluation. (Refer to the configuration guidance from the manufacturer to make these selections).

(U) Secure Logging

- Use a remote audit server (e.g., Syslog server). Protect the integrity and confidentiality of audit data through establishing an IPsec VPN connection between critical network devices and an audit server.
- Ensure that all network infrastructure devices create an audit event when configuration changes are applied, when operating system firmware is upgraded, and when the device is rebooted.
- Ensure that logs are reviewed on a regular basis.

3. (U//FOUO) For further information, please contact your IAD Client Advocate. Military commands/services/agencies should call 410-854-4200, and Civil and Intelligence agencies should call 410-854-4790.