



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

Supplemental Guide to the National
Manager's Letter

Introduction

Protecting National Security Systems (NSS) against unintentional and intentional compromise of confidentiality, integrity and availability are critical to the defense of our nation. National Security Directive 42 (NSD-42) and Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information) mandates the National Manager develop effective technical safeguarding policies and standards that address the safeguarding of information within NSS and assess the overall security posture of NSS. The National Manager assesses the progress of the NSS community in meeting minimum baseline requirements using Federal Information Security Management Act (FISMA) data, and other existing processes and data feeds, as available.

National Manager Baselines

Building on the themes of the 2012 and 2013 National Manager baselines, which focused on automated identification of devices and software in the environment and Secure Configuration Management, for 2014, the National Manager has established *credential management* and *access control* as baseline requirements to harden and defend NSS. The intent of the 2014 baseline is to strengthen and protect the credentials used to authenticate and access NSS systems. Efforts should be focused on employing effective authentication mechanisms, and protecting privileged credentials and accounts linked to critical mission capabilities. Properly implemented, the National Manager baseline requirements will improve an enterprise's security posture.

National Manager Guidance for 2014

NSS organizations should implement the following guidance at a minimum. This supplement provides guidance in priority order based on effectiveness in countering/containing adversary impact. Planning is underway to implement large-scale attribute and policy based access control solutions using enterprise-level subject attribute services and/or tagging of information in digital policies (see "Future Activities" below). The following guidance focuses on near-term activities achievable today.

Controlling Credentials and Access

Administrative privileges on a computer system allow access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted. When administrative privileges are improperly managed, granted widely, and/or not closely audited, attackers are able to exploit them and move effortlessly through a network. In addition to controlling administrative privileges, robust authentication and granular access control for all users further restricts the ability of an adversary to find and access resources.

- **Conduct Full Review of Administrative Privileges**

Review accounts with privileged / administrative credentials consistent with CNSS issuances and other efforts across the NSS community.

- **Follow the Principle of Least Privilege**

Define separate privileges related to different administrative tasks, grant users only those privileges necessary to perform duties within their roles, and protect privileged credentials by restricting how and where they can be used. Identify the few users who require domain administrator credentials and domain administrator logons; separate these accounts from typical administrative accounts using user groups with different privileges.

- **Ensure Privileged Accounts Do Not Have Email Accounts or Internet Access**

Restrict privileged accounts from performing general tasks such as accessing emails and browsing the internet whenever possible. Additionally, on servers, disable/remove browsing and email capability if not necessary for the server applications to function.

- **Remove Standard Users from the Local Administrators Group**

Do not grant standard user accounts membership in the local Administrators group.

- **Do Not Allow Access to Local Accounts Across the Network**

Remove network and remote interactive logon privileges from local, non-service, and administrator accounts. If physical administration is not possible, restrict remote logon to a select few privileged users from well-secured workstations.

- **Restrict Systems that Privileged Accounts Can Access**

Limiting general administration tasks to secure systems reduces the risk of exposure of privileged credentials. Establish physically separate network segments for administrative functions, including developing clean baseline images, configuration settings, and policies. Use private VLANs with port restrictions to prevent communication between hosts on the same subnet wherever possible. Enforce access restrictions using network- and host-based firewall rules and policy settings to restrict workstation-to-workstation communications.

- **Use Multi-Factor Authentication**

Use a robust authentication process and, for all privileged accounts at a minimum, require at least two-factor authentication. CNSSD 506 (National Directive to Implement PKI for the Protection of Systems Operating on Secret Level Networks) requires that public key infrastructure (PKI) issuances of two-factor (hardware and PIN) access credentials be deployed in 2014. Ensure privileged accounts are transitioned as soon as possible in this deployment.

- **Manage Passwords Effectively**

As multi-factor mechanisms are deployed, password-based logons to accounts should be disabled. During the transition and for accounts that cannot support PKI-based logon, passwords should be of sufficient length and complexity, with a combination of letters, numbers, and special characters. Consider using longer passphrases instead of traditional passwords. Require regular password changes for all accounts, especially privileged accounts, and train users to ensure that passwords are different from other accounts. Ensure unique, local administrator credentials are used on each machine. If passwords are stored for emergency access, keep these in a protected off-network location, preferably in a safe.

- **Effectively Protect Data**

Review content contained on information sharing portals (both classified and unclassified) to identify information that should not be shared with the full user population. Information content found to be sensitive should be removed as soon as possible, or access removed, until appropriate authentication mechanisms are in place.

Review information sharing portals on classified networks to ensure each requires authentication and system event logging.

Future Activities

- **Credential Management and Access Control**

Credential Management and Access control are essential capability areas being explored in ongoing NSS activities to establish and sustain network security. Active Directory (AD) structures, Access Control Lists (ACLs), and other types of access controls are all part of robust access control solutions in the near future. While AD and ACLs may be sufficient to protect some information, they may not, by themselves, give an organization the flexibility needed to balance the need to know with the need to share. Other forms of access controls such as role based access control (RBAC), policy based access control (PBAC) and attribute based access control (ABAC) will also be useful for some applications and will

expedite movement of information to cloud technologies while still affording this information access control protections.

Since most human resources and security departments have processes for gathering information about employees who will be users of systems, start thinking about how this HR or Security information could be used for access control. You will need to determine if the information has the quality and timeliness to be used for access control and if the data is considered to be authoritative. Also, do you have the ability to automatically update and use these attributes of users (HR and Security and other sources of authoritative information like training information) in an access control decision for access to systems or critical resources? Thinking about these things begins to position your organization to ensure that users have access to the information they need to do their jobs effectively, while still allowing sufficient sharing of and protections for information.

In addition the ability to tag your information will allow finer grained access to sensitive information. Start thinking about how you will create the tags needed to accomplish this type of access control. Using the characteristics of the information, there are many possible strategies for developing tags.

Some of the questions that will better position your organization for finer grained information-driven (data-driven) access control solutions are:

- What are the policies, laws and regulations that determine who can access your systems or critical resources managed by those systems?
 - What are the attributes for users and resources that are needed to implement these policies, laws and regulations? Make a list of these. Can you write English policy statements about who can access different types of information and critical resources on your systems that can be easily converted into a digital form of the policy?
 - Does an authoritative source for these attributes already exist somewhere in your systems (HR or Security, Other)?
 - Is there a standardized definition and format for these attributes recognized across CNSS, or used by one or more of the member organizations that you can use within your system?
 - Is there a standardized definition and format of the resource attributes (data attributes) recognized across CNSS or used by one or more of the organizations for tagging your data?
 - Does an individual (or a member of a group) associated with a mission attribute or mission role have the operational authority to access specific information, information services, or participate within information transactions?
 - What types of data are critical to your mission and who is authorized to access this data? The following questions can be used to characterize your information: Where is the information coming from? Who owns the information? What format is the data in? Is the information classified or sensitive? What authorizes your organization to hold and use the information? Who can the information be shared with (only specific individuals, anyone in your organization, everyone in your agency, external entities outside your agency)?
 - What can a user do once they access a type of data (can they copy it; change it)?
- **Other Future Activities**
- Many departments and agencies are also exploring cloud technologies, thin client, and data-level security implementations. New architectural concepts are being employed with these technologies to collapse network security boundaries, reduce the external attack surface, secure information sharing with mission partners, and integrate interoperable, large-scale Identity, Credential and Access Management

(ICAM) solutions. The baseline requirements and future activities in this letter form a foundation for these innovations which will be expanded upon in subsequent years.

Information Resources

The Information Assurance Directorate (IAD) provides a number of additional documents that address NSS baselines and other capabilities. These can be found at www.nsa.gov/ia/mitigation_guidance/ and include the following areas (those most applicable to this guide are highlighted in bold):

- Application Whitelisting
- **Control Administrative Privileges**
- **Limiting Workstation-to-Workstation Communication**
- Antivirus Cloud
- Anti-Exploitation
- Host Intrusion Prevention System (HIPS)
- Secure Baseline Configuration
- Web Domain Name System (DNS) Reputation
- Take Advantage of Software Improvements
- **Segregate Networks and Functions**

These best practices are part of the **Community Gold Standard (CGS)**. CGS is a framework to provide security best practices across governance, protection, detection, and resilience related capability areas. CGS information can be found at: www.iad.gov/iad/CGS/cgs.cfm

For additional mitigation guidance or general IA Guidance, please contact NSA at NIASC@nsa.gov. To get involved in the Community Gold Standard effort, please contact the CGS team at CGS@nsa.gov.

Ensure that your enterprise remains current with the latest policies, instructions, directives and standards released from the below sources. Working groups continue to develop/update policies and standards to secure NSS, such as the soon to be released CNSSD 508 – Security-Focused Configuration Management and updated CNSSD 504 - Protecting National Security Systems from Insider Threat, and under development, a Privileged User Annex.

- Committee for National Security Systems: <https://www.CNSS.gov>
- Intelligence Community: <http://www.dni.gov/index.php/about/organization/chief-information-officer/ic-cio-enterprise-integration-architecture>
- National Institute for Standards and Technology: <http://NIST.gov>
- Information Assurance Support Environment: <http://IASE.disa.mil>