NBS Security Brief

NIH IT Security

NIH approaches IT security from several different directions: a master security plan that provides guidance as to policies, technologies and practices designed to enhance the security of all NIH IT systems; individual security plans that deal with specific issues of each enterprise IT system; a wide range of training and awareness resources; physical and logical barriers to intrusion, and tools that monitor and measure the strength and health of the security measures. Information regarding the overall NIH security approach is presented at several web sites. Try http://www.cit.nih.gov/security.html as a starting point, and http://irm.cit.nih.gov/nihsecurity/secfaqnih.htm for a set of FAQs.

The Master Security Plan establishes the methodology and format for all NIH System Security Plans, and serves as the agency-wide security guidance. In turn, and consistent with the policy, procedures and rules described in the NIH Master Security Plan, NBS has written and implemented its own Security Plan. The NBS plan is intended to further delineate and highlight the security policies and specific rules that the system, and each of its users, must follow.

The NBS System Responsibilities

The NBS utilizes various methods to monitor, test and control the following:

Identification and Authentication - hinders unauthorized access to the NBS. Identification is the means by which a user provides a claimed identity to the NBS, and authentication is the means by which that identity is confirmed. The NBS means of identification and authentication include:

- For general web-access, the NBS will utilize NIH's Login service. Each NBS Application (Oracle, Gelco, etc.) delegates its authentication to NIH Login service. Currently, NIH Login uses a password to verify identity. To avoid multiple individual systems requiring different usernames, different passwords and different user administration interfaces, NBS authentication is managed enterprise-wide by NIH Login.

- For operating system-level access CIT Operations follows strict account management and access guidelines.

- Password System - The NIH password policy can be found at the NIH Policy on Passwords website, http://irm.cit.nih.gov/policy/passwords.html Guidelines for choosing strong passwords can be found on the CIT website at http://irm.cit.nih.gov/security/pwd_guidelines.html . NBS users are educated about the importance of strong passwords through the NIH Computer Security Awareness Training Web Course at http://irtsectraining.nih.gov/.

Intrusion Testing - the NIH Incident Response Team conducts all penetration tests on NIH networks.

Intrusion Detection - monitors the network to detect attacks or other security related events and notify security personnel of suspicious network activity.

Review of Audit Logs - records showing who has accessed a computer system and what operations were performed during a given period of time.

Access Controls – (Authorization) automated mechanisms used to regulate access to a specific system resource and the type of access that is permitted. Oracle provides tools to limit users' actions on the system to the least privileged access required for a job function.

Separation of Duties - delegation of authority in a manner that divides authority and responsibility among more than one person (the person who writes the check can't approve it).

New Account Procedures – Requests for new user access are controlled by the ICs and monitored by the NBS.

Remote Access - There will be no general user access to the NBS environment outside of NIHnet (But NIH's Parachute dial-in facility allows individuals to become part of NIHnet from remote locations.)

Discontinuing Account Access – NBS user access will be disabled after six months of inactivity.

Failed Authentication Attempts - Three failed log-on attempts result in disconnection.

Session Timeout– an automatic session timeout feature terminates user connections after sixty minutes of inactivity.

Network Access/Encryption – Encryption is utilized between users and servers.

Firewalls - NBS also employs firewall software to protect the information contained in the system.

Internal Security Labels - NBS electronic media, including any storage media that contains sensitive information such as word files, paper documents, and removable media are labeled to indicate the level of sensitivity.

Log-on Banner - Public Law 99-474 requires a warning message be displayed that notifies unauthorized users that they have accessed a U.S. Government computer system and explains the resulting punishment for unauthorized access.

Data Integrity/ Validation Controls - Integrity of data and network security is the assurance that information within a system is reliable and accurate. Integrity controls are used to protect the operating system, applications, and information in the NBS from accidental or malicious alteration or destruction and to assure the user that the information meets expectations about its quality. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

Virus Detection and Elimination - Virus detection and elimination software is installed on file servers, email servers, and workstations. Virus protection software is run periodically on all servers and workstations and virus definitions are updated frequently. Virus protection software is updated and upgraded on a regular basis. Virus protection is provided at the following levels: 1) NIHnet Perimeter Level Protection; 2) Server Level Protection; and 3) Desktop Level Protection.

User Responsibilities

Computer security is the responsibility of everyone who can affect the security of a computer system including the end user. Within the NBS there are two kinds of users, and their associated responsibilities are described below.

Users of Information. Individuals who may only read or be briefed on computer prepared reports. Some users of information may be very far removed from the computer system. Users of information are responsible for letting the functional managers/application owners know their needs for the protection of the information, especially for its integrity and availability. These users are also responsible for appropriate protection of information they receive from the system.

Users of Systems. Individuals who directly use NBS are responsible for following NIH security procedures, for reporting security problems, and for attending required computer security and functional training.