Overview of NBS System Security

When designing the NIH Business System (NBS), including the Travel module, the NBS team was concerned with protecting extremely sensitive user data, such as social security and credit card numbers. To protect this data from computer viruses and malice, the team implemented multiple levels of system security, from both the client and server sides, as well as NIH-wide. Subsequently, the NBS was rigorously tested to certify that the security measures were effective. The NBS security plan is consistent with the policy, procedures, and rules required in the NIH Master Security Plan. The NIH CIO has certified the NBS plan accordingly. The following paragraphs outline some of the security protection mechanisms that are in place.

Protection while Logging in and Transmitting Sensitive Data

The NBS is accessed securely via a web browser, such as Internet Explorer or Netscape. After the user logs in with his/her NIH ID and password, the web browser automatically encrypts all data before sending it across the network to the servers, and back to the user's computer.

Protection for Data Stored on the Servers

Once data is transferred to the NBS, it is protected physically and at the application level:

- The NBS servers are locked in a secured server room with restricted access;
- Firewalls reside in front of the servers to restrict access;
- The databases that store the data are configured to provide only minimal access and to protect all data;
- Only authorized users have access to the NBS;
- The concept of "Separation of Duties" prevents system administrators from gaining un-authorized access to the NBS Travel System,; and
- Vulnerability assessments are conducted regularly to quickly identify and correct any new security "holes."

Protection from Systems Outside of NIH

Access to the NBS Travel System is restricted to computer systems within the NIH firewall; however, NIH users may remotely access the NBS Travel System by connecting through their Parachute account or VPN client. Intrusion detection software constantly monitors the NBS, looking for any un-authorized attempts to gain access to or modify user data.

Conclusion

It is important to remember that security is ultimately everyone's responsibility. The NBS Team has taken many steps to protect the NBS and its users. NBS users can supplement this security by changing their passwords regularly and not sharing them with anyone. By working together and maintaining security awareness, we can substantially reduce the risks from malicious users, viruses, and worms.

If you would like more technical information about NBS security measures, select NBS Security Brief.