What was NSA's involvement in producing Windows Vista security guidance?

As with previous efforts on Windows Server 2003 and Windows XP security guidance, NSA's Information Assurance Directorate (IAD) worked closely with Microsoft and various government agencies to come to consensus on security settings desirable for sensitive and traditionally high security network environments. NSA personnel worked hand-in-hand with Microsoft and various government organizations to conduct product research and testing and provide recommendations to Microsoft for inclusion in the "Specialized Security – Limited Functionality" (SSLF) security settings. We believe that the SSLF settings closely mirror what we would have recommended had we written our own guide.

Has NSA "approved" the use of Windows Vista and Internet Explorer 7 on government systems?

NSA has not approved or disapproved the use of Windows Vista or IE 7 on government systems. Each organization is responsible for establishing and following its own policy regarding approved software. However, via the Microsoft security guide, we have provided recommended best practices for securing Windows Vista and IE should an organization decide to deploy the operating system.

Should I deploy the SSLF policy "as is" on my Windows Vista systems?

SSLF security settings are an excellent starting point for securing Windows Vista systems. Additionally, Microsoft provides an automated tool for creating SSLF Group Policy Objects (gpoaccelator). However, we strongly recommend that organizations carefully review each setting and customize according to the unique operational constraints of their networks. In some cases, the Enterprise settings in the Windows Vista security guide may be more desirable. Additionally, careful testing on non-production and non-critical systems prior to wide-scale deployment is essential.

With which organizations did NSA partner in the development of Windows Vista security guidance?

In addition to Microsoft, NSA partnered with DISA, NIST, and the U.S. Air Force in the actual security settings decisions. Since then, NSA has established additional partnerships with U.S. Navy, U.S. Marine Corps,

U.S. Army, Department of Homeland Security, and the Office of Management and Budget that have focused on developing standard Windows Vista desktop configurations.

How do the SSLF settings differ from those in the DISA STIGs or the military service standard desktop configurations for Windows Vista?

For the past several years, NSA has partnered with the U.S. Air Force (USAF) in the development of standard security configurations for USAF Windows systems. In late 2006, a standard baseline for all USAF Windows Vista machines was agreed upon by representatives from various commands and organizations within USAF. Leveraging the work done by the Air Force, both the Army and Navy/Marine Corps pursued similar initiatives to establish standard Windows Vista configurations. Vista configurations for the military services are based off of the Microsoft Windows Vista security guide's SSLF recommendations, with some deltas based on operational constraints. Realizing that the configurations proposed by the various services were strikingly similar, representatives from each service met to finalize security settings to be incorporated into a Windows Vista Department of Defense standard desktop configuration (SDC).

The DISA Security Technical Implementation Guide (STIG) for Windows adopts the SSLF recommendations with a few exceptions noted in a DISA addendum. DISA, NSA, and Microsoft will take the results of the DoD SDC meeting to work on more closely aligning the DISA STIG and Microsoft SSLF guidance with the agreed upon configuration. Thus, future version of Microsoft's SSLF guidance may reflect minor changes.