June 2003

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

ASSET: SECURITY ASSESSMENT TOOL FOR FEDERAL AGENCIES

Elizabeth B. Lennon, Editor, Information Technology Laboratory, National Institute of Standards and Technology

Based on the Federal IT Security Assessment Framework, ITL's governmentwide information security assessment tool, Automated Security Self-Evaluation Tool (ASSET), assists federal agencies in improving the security of their information systems and resources. ASSET automates the completion of ITL's security questionnaire, which was published in NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems*, by Marianne Swanson. Guidance from the Office of Management and Budget directs federal agencies to use this document as the basis for conducting their annual reviews under the Federal Information Security Management Act (FISMA). Through interpretation of the questionnaire results, users are able to assess the IT security posture for any number of systems within their organization and, in particular, assess the status of the organization's security program plan. This *ITL Bulletin* describes the features and capabilities of ASSET, which is freely available at http://csrc.nist.gov/asset.

The Assessment Process

The Federal IT Security Assessment Framework identifies five levels of IT security program effectiveness. Each level contains criteria to determine whether the level is adequately implemented. Once the degree of sensitivity of information has been established, the asset owner determines whether the measurement criteria are being met. Benefits of the framework include identifying a standard way of performing self-assessments and providing flexibility in assessments based on the size and complexity of the asset.

Assessment refers to the entire process of collecting and analyzing system data. The assessment process involves three steps:

- Data collection – the process of gathering and entering system data
- Reporting – creating aggregate data so that it can be analyzed
- Analysis – the process of understanding, evaluating, and making judgments upon a set of system data

ASSET supports the assessment process by facilitating the data collection and reporting steps of the process. It is important to note that ASSET can be used to assess one or more systems or an entire security program in terms of the five levels of IT security program effectiveness established by the framework.

Roles and Responsibilities

Within the assessment process, roles and responsibilities need to be clearly defined.

The *manager* is the individual(s) with primary responsibility for the assessment. This individual is responsible for analysis of the results. The manager is often the CIO or program official within the organization.

The *reporter* is responsible for importing multiple system data into ASSET. This individual must fully understand the deployment, installation, and execution of ASSET. The reporter ensures that all questions are answered for all systems and aggregates results from all systems within an agency or enterprise. The reporter also generates all reports.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since January 2002

The *collector* ensures that all questions are answered for each system under a collector's review. This individual(s) interacts with the subject matter expert to gather system information and clarifies data as necessary. The collector enters individual system data into ASSET. A typical assessment will have multiple collectors and one reporter.

The *subject matter expert (SME)* must be knowledgeable about the system or topic areas (i.e., physical security) being assessed. This individual provides specific responses to assessment questions. The subject matter expert interacts with the collector on an as-needed basis.

ASSET Scope

ASSET assists in gathering data and reporting results for IT systems. It is a stand-alone java-based software application, which requires that users be responsible for the security of the data (host-based security). ASSET is not a web-based application (client:server). It does not establish new security requirements, analyze report results, or assess system or program risk.

ASSET Architecture

ASSET is comprised of two separate host-based applications: ASSET-System and ASSET-Manager.

ASSET-System:

- Provides for data entry and storage of individual system data;
- Generates single system summary reports, for the user who completes the questionnaire, providing immediate picture of single system assessment results; and
- Tracks all collectors and SMEs who provide answers to ASSET questions.

Within ASSET-System, the questionnaire is presented in a progressive format, allowing users to move backward and forward in the questionnaire at their discretion. ASSET-System allows users to return to the assessment of a particular system, by saving the prior status of the assessment.

Once the assessment is completed, a user can locally generate summary reports of individual systems giving an immediate picture of the assessment results. Reports can be exported to any popular spreadsheet or charting program. Reports provide:

- A summary of topic areas by levels of effectiveness;
- A list of N/A questions;
- A list of risk-based decisions; and
- A system summary.

ASSET-Manager provides the ability to sort and summarize the questionnaire results for all systems assessed and to display the results through several formatted reports or through an export capability.

ASSET-Manager:

- Aggregates data from multiple systems so that agency-wide reports can be developed; and
- Tracks all collectors and SMEs who provide answers to ASSET questions.

ASSET-Manager is intended to generate reports, exportable to any spreadsheet application, that are interpreted by the managers who request an assessment. Reports provide:

- A summary of all systems;
- A summary of system types;
- A summary by system sensitivities; and
- A summary by organization.

ASSET Installation Minimum System Requirements

- Hardware – Pentium II – 266 MHz processor
- Operating systems – designed to operate on all Windows 9X operating systems; initial operating capability on W2000 Professional
- Memory requirements – 120 MB free space.

Following Windows conventions, the ASSET installation wizard guides the user through the installation process.

ASSET Information Security Considerations

Agencies should determine data and report sensitivity, and are responsible for data protection. ASSET does not provide for any security of data, such as encryption, while the data is stored or in transit. Application-based security is not provided for data transmitted between data collector and reporter. Since it uses Microsoft SQL Server Desktop Engine (MSDE), ASSET has the vulnerabilities of MSDE. Users should mitigate these vulnerabilities before using ASSET. Finally, as a best practice of all assessments, ASSET-System should be uninstalled after an assessment is completed.

Access controls are provided by operating system login requirements. New ASSET user accounts are created when ASSET is installed. Login consists of user name and e-mail address. No password protection is provided for accessing the application or data.

Since data collection efforts represent a substantial expenditure of labor, agencies should determine and implement an appropriate backup strategy. ASSET saves the current file on specified intervals but does not provide automated backup of data.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

Conclusion

ASSET-System and ASSET-Manager work together to assist agencies in collecting and reporting IT security self-assessment data. Federal agencies are now utilizing the ASSET software tool to automate the collection of system data and the creation of reports in conducting annual reviews to satisfy the requirements of FISMA. In testimony given on November 19, 2002, before the Congressional Committee on Government Reform, the Associate Director for Information Technology and Electronic Government, Office of Management and Budget, described eight achievements that had improved the federal government's IT security in 2002. One of the achievements was ITL's development of ASSET. The ASSET software and all documentation, including NIST SP 800-26, are available at http://csrc.nist.gov/asset.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900