STACS Features & Services

Assessments

All participating offices take part in an Internet-based assessment every year. This assessment provides the baseline data that drives the STACS program. Using a web-based questionnaire, offices describe their IT infrastructure and procedures. The data collected is used for various reasons: to support the help desk function, to select offices for further assessment, to produce aggregate reports for the NACTT, and to provide input to the mitigation process, to name a few.

Over one third of participating offices have an onsite assessment each year. This activity is designed to evaluate the IT inventory, identify security problems, address individual issues, produce a written report for the office, and answer questions from the Standing Trustee or office IT specialist.

Over the life of the STACS contract, every office will receive an onsite assessment at least once every third year.

Vulnerability Scanning

The STACS support center scans the Internet connections of participating offices to look for known security vulnerabilities and to identify inbound paths (ports) that should normally be closed. When these exposures are identified, the support center works with the office to help them make corrections. This scanning process takes place semi-monthly to detect inadvertent or intentional changes.

The office telephone lines are also called periodically to identify modems that might let an intruder gain access from outside the office.

Reporting

Reports are provided to document the findings of assessments and to present recommendations for improvement. Aggregated data is summarized and provides a basis for developing recommendations for best practices.

Statistical reports are prepared monthly for the NACTT to help track the overall progress of the program. Aggregate data is used to construct long term improvement campaigns to reduce the IT security exposures in participating offices.

Best Practices and Model Policies

The STACS support center reviews assessments and industry data sources to develop a collection of best practices for participating offices. Model policies have been developed to allow offices to quickly design and implement policies for IT issues.

The model policies are adaptable to local needs. Where appropriate, they contain alternative policy choices to allow each office to quickly customize the document to local needs. Online training mirrors the standards outlined in these model policies.

Web Enabled Database

The primary information delivery mechanism for the STACS program is the STACS web site at **`www.stacs.net`**. Participating offices are able to obtain information about a wide range of topics directly from the web site. These include examining and updating their assessment data, querying known vulnerabilities, and reviewing best practices, among many other features.

Access to the web site is protected by encryption and passwords.

Training

A key element of the STACS program is the provision of online and live training for participants. Online training courses address the needs of several audiences within the Standing Trustee community, including office personnel and management staff.

Training has been adapted and expanded over time in order to implement the improvement goals of the STACS program. Interactive and self paced web based training is used for most purposes, and is tracked to determine participation levels and attainment. Onsite training will be offered in conjunction with regional NACTT functions to reduce travel expenses for attendees.

The STACS program also provides an electronic newsletter that contains articles on security topics of interest to the community.

Vulnerability and Patch Alerts

The STACS support center provides participating offices with customized alerts for new security vulnerabilities and significant vendor-issued patches. On a daily basis, the support center reviews alert notifications sent by a commercial security service. After reviewing this raw data, the STACS support center evaluates its applicability to the Standing Trustee community. Alerts of interest are updated to include recommended action and are sent to participants.

Once the web-based assessments are completed, they are used to filter the alert messages so that offices only receive alerts of interest. Users also have the ability to search the STACS web site for data on past alerts and vulnerabilities.

Consulting Assistance

The STACS program is designed to provide a range of general resources directly to participating offices. Nonetheless, each office may identify needs that require live assistance. The STACS program offers each participating office personalized consulting support.

Consulting support can be used for virtually any purpose related to IT security. For example, a participating office might rely on the STACS support center to review a vendor's proposal for equipment upgrades. The support center could offer guidance concerning the security aspects of the equipment or might suggest additional security-related services to be provided by the vendor.

The STACS program will track and report monthly the amount of consulting time provided to each participating office.

Emergency 24×7 Support

In the event of a security emergency, participating offices can contact the STACS support center at any time. An on-call support representative will call the affected office to provide support.

Incident Response

In the event of a substantial IT security breach, the STACS program will send security specialists onsite to provide assistance in handling the incident. This assistance could include services such as limiting further damage, documenting the incident, and recovering key servers.

There is a limit on the number of times this service will be provided, which will vary with the overall level of participation in the program.

Optional, Separately Priced Services

Participating offices can arrange directly with the STACS contractor to provide optional, individual services beyond the base services included in the STACS program.

This document provides an overview of the basic STACS program services. The authoritative description of these services, including limits on quantities, is contained in the master contract.

Rev: June 19, 2007