



## ITL SECURITY AUTOMATION PROGRAM

NIST, in coordination with the National Security Agency, Department of Defense, Department of Homeland Security, and industry partners, has developed technical specifications for sharing security information between information systems. NIST is providing security vulnerabilities and metrics, IT product configurations, and compliance mapping reference data sets to the areas of vulnerability and configuration management, collectively known as security automation.

Security Automation comprises a suite of specifications for organizing, enumerating, and expressing security-related information in standardized ways. Security Automation and associated reference data can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking systems security configuration settings, and examining systems for signs of compromise. In addition to configuration, patch, and compliance use cases, security automation specification data is also being leveraged to solve problems related to software and asset inventory, malware detection, and event correlation.

Security automation reference data is currently housed at the National Vulnerability Database (NVD). The NVD is the U.S. government repository of standards-based vulnerability management data using security automation specifications. This data provides a standards-based foundation for the automation of vulnerability and security configuration management, security measurement, and compliance. The NVD includes databases of security checklists for the National Checklist Program (NCP), security-related software flaws, misconfigurations, product names, and impact metrics.

The Web site is: <http://scap.nist.gov>