# Glossary for the Information Security Automation Program and the Security Content Automation Protocol

**SCAP content**: consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

**SCAP checklists**: are configuration checklists written in a machine readable language (XCCDF). SCAP checklists have been submitted to, and accepted by, the NIST National Checklist Program. They also conform to an SCAP template to ensure compatibility with SCAP products and services. The SCAP template discusses requirements for including SCAP enumerations and mappings within the checklist (see below).

**SCAP test procedures**: SCAP checklists reference "SCAP test procedures" for machine readable information on performing low level checks of machine state (OVAL). SCAP test procedures are used in conjunction with SCAP checklists.

**SCAP enumerations**: include a list of all known security related software flaws (CVE), a list of known software configuration issues (CCE), and a list of standard vendor and product names (CPE).

**SCAP mappings**: interrelate the enumerations and provide standards based impact measurements for software flaws and configuration issues. Thus, for any given software flaw (CVE) one can determine the affected standard product names (CPE). For any given standard product name (CPE), one can determine the configuration issues that affect that product (CCE). For any given software flaw (CVE) or configuration issue (CCE), one can determine the standard impact score (CVSS).

**SCAP check**: a specific configuration check within an SCAP checklist. Note that checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

**SCAP reports**: are the results produced from evaluating an SCAP checklist against a target. SCAP reports are required to include SCAP enumerations and mappings per the SCAP template.