Form 3 Mandatory Requirements and Form 4 Rated Requirements

					Vendor	
MANDATORY		Primary Function	Secondary Function		Met	Comment
M1	The solution must fully support implementation, administration, configuration and scanning for both IPv4 and IPv6 networks.					
M2	The solution must be capable to perform assets discovery scans and vulnerability scans of 2,000,000 devices at minimum. A discovery scan must record 10,000 IP addresses in one day. A full non-credential based scan of 10,000 IP addresses must complete over a 2 day period, staggered over non-production hours to limited impact to daily operations. A full credential based scan of 10,000 IP addresses must complete over a 3 day period, staggered over non-production hours to limited impact to daily operations.					
M3	Communications between manager, scanners, agents, and reporting tools must have configurable time intervals with time stamping of communications.					
M4	The solution must be capable of Risk Prioritization customization based on business context.					
M5	The solution must be capable of Risk Prioritization customization based on CVSS.					
M6	The solution must have the ability to ingest vulnerability scan results from other vendors in either various formats.					
M7	The solution must have the ability to consume and execute industry or custom SCAP 1.2 or later content.					
M8	The solution components must be available as software and hardware based appliances.					
M9	The solution must maintain and store secure audit logs in accordance with GC policies. (See http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742)					
M10	The solution must uniquely identify and track all discovered assets, including software and firmware, hosted on GC infrastructure.					
M11	The solution must be capable of processing, communicating, and storing data using a GC approved encryption method where deemed necessary (i.e. data sensitivity) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or in a subsequent version;					
M12	The solution must provide detail remediation prioritization. Provide analysis and recommendations on which vulnerabilities to focus on first.					
M13	The solution must uniquely identify and authenticate organizational users through the use of Microsoft Active Directory Services.					
M14	The solution must provide a VA scanning component that is capable to scan Virtual Machine, non-Virtual Machine and Cloud environments.				.	
M15	The solution must provide software based scanners with built-in management consoles, which can operate as stand-alone when disconnected from a management server.					

					Vendor	
MANDATORY		Primary Function	Secondary Function		Met	Comment
M16	The solution must enforce a trusted/authenticated relationship with the source of vulnerability information.					
M17	The solution must have the ability to interface with the vulnerability information from the National Vulnerability Database (NVD) for data feed sources.					
M18	The solution must have the ability to back up its entirety which includes, but not limited to, scan data configuration.					
M19	The solution must permit patches and updates to its toolset to be deployed in various approved ways including, but not limited to, over network, USB, and downloadable.					
M20	The solution must provide the ability to ensure that all logs/debugging information/memory dumps can be sanitized for sensitive information so that they may be shared for vendor support.					
M21	The solution must have Common Criteria certification at EAL3 or higher to ensure product has been adequately tested and reviewed.					
M22	The solution must be capable of performing agent and agentless scanning of configuration compliance.					
M23	The solution must support configurable, scheduled, and ad-hoc scanning.					
M24	The solution must be capable of performing agent and agentless scanning for vulnerabilities.					
M25	The solution must be capable of conducting both unauthenticated and authenticated VA scans.					
M26	The solution must provide a method of excluding hosts or host groups from being scanned (IP range, dynamic asset groups, etc.).					
M27	The solution must provide asset discovery, grouping, and management and classification capabilities.					
M28	The solution must be capable of delivering configuration compliance scans.					
M29	The solution must provide a central repository of reports with numerous report output formats, including but not limited to PDF, HTML, XML and CSV.					
M30	The solution must provide a PCI compliant security standard template.					
M31	The solution must provide updates for industry recommended and standardized scan templates.					
M32	The solution must also allow for the ability to create, modify and customize scan template options such as ports, protocols, and network packet behavioral characteristics used for scanning.					
M33	The solution must have configurable role based access.					
M34	The solution must have the ability to conduct credential and non-credential scans using the least privileged access privileges for credential based scans.					

					Vendor	
	MANDATORY	Primary Function	Secondary Function		Met	Comment
M35	The solution must be able to control a scan in a remote location over a slow network link of 512K. The solution must also be able to report the scan results and record information from that remote location into database at the central location.					
	RATED REQUIREMENTS					
R1	The solution should support centralized management and reporting servers which can operate independently (including their respective dependant scanners and agents), as well as be subordinate to a higher echelon of management and reporting servers. The management and reporting servers should support multiple hierarchal levels of subordinate management and reporting servers (including their respective dependant scanners and agents).				10	
R2	Solution should support storage of credentials in a FIPS140 validated Hardware Security Module.				5	
R3	The ability to provide customizable grouping, management and classification capabilities of assets.				5	
R4	The ability to group multiple IP addresses into one asset.				5	
R5	The vulnerability database signatures updates should be available for use by the system within 6 hours of release.				5	
R6	The ability to integrate with SIEM technologies using the following audit outputs and protocols. Audit output: Text file, rolling text file and Comment Event Format (CEF). Authentication protocols to collect file: SAMBA, FTP (SFTP), database using JDBC driver, syslog, HP SmartConnector ready, CEF ready events and Log event Extended format (LEEF).				10	
R7	The ability to send automated email notification to configurable recipients.				5	
R8	The ability to scan target platforms - SSC existing standards are (non-exhaustive list): Windows, Redhat, CentOS, Debian, Ubuntu, Fedora, FreeBSD, SUSE, Mac OSX, AIX, Solaris, HP/UX, Cisco IOS, F5, SCADA. 1 point each, max of 10 points				10	
R9	The ability to integrate with common change/workflow management platforms to automate the generation of external workflow and ticketing. Provide listings of supported systems. 1 point each, maximum of 5 points				5	