The CCSF information security infrastructure is improved on an ongoing basis to incorporate vendor feature enhancements, adapt to new threats and provide the necessary capacity to meet the needs of Instructional and Administrative programs. A defense-in-depth model is followed consisting of multiple firewalls, desktop anti-virus solutions and employee security precautions. CCSF uses a Checkpoint firewall as the primary security system. It was upgraded in April, 2012, and an Intrusion Prevention System (IPS) software blade was activated. The IPS feature is one of the most recent improvements in the field of network security and provides a dynamic method of preventing malicious activity. CCSF also uses a secondary firewall from Palo Alto Networks for additional security. It was upgraded in June, 2012 and is currently used for controlling peer-to-peer (P2P) traffic, conducting threat analysis and performing anti-virus filtering. CCSF has a site license for McAfee Anti-Virus software which is used for Faculty, Staff and Student desktops. The site license provides access to the latest versions of software on an ongoing basis. Replacement anti-virus solutions are being evaluated and tested with the goal of selecting a new anti-virus solution during the first quarter of 2013. The improved desktop computer replacement cycle of a maximum of five years will provide sufficient performance capacity to utilize the capabilities of desktop anti-virus solutions. International standards will be followed when possible for future information security implementations as outlined in the Control Objectives for Information and Related Technology (COBIT) guidelines.

Reference:
Control Objectives for Information and Related Technology (COBIT):