# Security of the NSSE Computing Environment

The NSSE Institution Interface and Survey are programmed and administered by the Indiana University (IU) Center for Survey Research (CSR). The computing environment at the CSR requires a high level of computer and data security per the policies governing IU information technology resources and data. The University Information Technology Services Policy Office (UIPO) at IU provides a baseline level of enforced security requirements including protocols to prevent unauthorized access to IU computers. The CSR computing staff uses industry standard best practices as our security procedures. Each CSR workstation is updated daily with virus protection software. CSR endpoints are scanned daily for needed security patches and hotfixes. The centralized security server deploys all needed Microsoft security patches each night and machines are audited weekly to verify security patches are up to date.

The CSR employs the Principle of Least Privilege when assigning access rights to staff. The systems administration staff has designed a number of processes for preventing intrusions or data loss on the CSR's servers. Remote access to the servers is tightly controlled by user IDs and passwords. Physical access to servers is restricted per the security protocols of IU's data center. Access to directories on the file servers is restricted to only those employees who need to use them. Security processes similar to those run on the workstations are used to prevent, detect, and repair security problems on the servers. The servers are located on a private IP address restricting their access from the outside world. They also are behind a network firewall, and employ their own machine firewall. IU provides security scanning of our servers to look for possible problems and the computing staff carefully monitors server event logs for possible attempts at intrusions. Individual workstations are part of a Virtual Lan (VLAN) which allows even greater restriction of access. Any remote access requires a connection using an SSL VPN behind two-factory authentication.

The files on the servers are backed up each night, and the data is encrypted in the backup. The file and web servers are virtual systems employing RAID 5 technology to insure that a disk failure will not cause any loss of data. They are located in a modern class 4 data center designed to meet FEMA standards for surviving an F5 tornado. The building is staffed 24X7 and employs all modern physical security measures.

The CSR uses 2048-bit public key encryption with a 128–bit SSL connection to ensure the security of survey and other sensitive data that are transmitted across the Internet. The digital certificates were issued by InCommon/COMODO and are used by the survey respondent's browser to verify that the user is connected to the website that matches the name in the URL. The browser and the server then encrypt and exchange keys that are used to encrypt the remainder of the session. Through the use of these keys, the data are transmitted using the SSL. The security procedures used by the CSR are equal to or surpass the requirements for transmitting confidential information.