



## September 2014 NDSCS Data Exposure Update

Legislative Information Technology Committee – October 30, 2014

### Timeline:

Sept. 2.....Notified of malware present on about 150 computers.

Sept. 15....Found personally-identifiable information (PII) on 68 computers during malware remediation; contacted NDUS CIO for assistance.

Oct. 1 .....All PII located and matched to 15,6000 current and former students and employees.

Oct. 8 .....Letters mailed to all affected individuals.

Oct. 9 .....Public notification / press conference.

### Current Status:

- Analysis of computer and network logs by external forensic organization did not find evidence of any data exfiltration, but could not definitively rule it out.
- 125 individuals have contacted the incident call center (as of Friday, Oct. 24) in response to the letter or announcement.
- All administrative passwords to campus systems changed, access tightened.
- Malware detection software installed on all servers that store users' data.
- Research proceeding into deploying a malware solution and/or a more robust endpoint protection solution campuswide.
- PII scanning and encryption software selected and is currently being deployed (HR is complete; Business Office in-process; Enrollment Services next).
- New host firewall installed. VPN is being configured to improve the security of connections to the campus network and servers.
- ITD-deployed intrusion prevention/detection appliances installed on NDSCS' segment of the state network on Sept. 27.
- Meeting scheduled in early November with the NDUS Interim IT Security Officer to review NDSCS' IT security and to plan improvements.