



# Presentation to the Information Technology Committee

June 18, 2014

Grand Forks



**Lisa Feldner, NDUS  
Vice Chancellor of IT**



**Dan Sipes, ND ITD  
Deputy CIO**



## NDUS and ITD Security Coordination

- Over the last 4 Month NDUS and ITD have been working together to coordinate on high level security initiatives
  - Intrusion Detection/Prevention
  - NDUS Internal Review
  - Comparison of Security Processes and Procedures



## NDUS - ITD Security Comparison - SIMILARITIES

- **Endpoint Security**

- ITD and NDUS both manage local computers using automated configuration management tools and local Anti-Virus software.
- Advanced centralized firewalls for layered protection of end point devices.
  - ITD currently uses advanced firewalls to provide intrusion detection/prevention to all end point devices.
  - NDUS is currently implementing the same system to provide intrusion detection/prevention to all end point devices.



## NDUS - ITD Security Comparison - SIMILARITIES

- **Network and Data Center Security**
  - ITD and NDUS are using a variety of similar network monitoring systems to provide layered security to the network.
  - ITD and NDUS use data encryption technologies to ensure the secure transport of data.
- **Vulnerability Scanning**
  - ITD and NDUS are using the same vulnerability scanning system to proactively scan servers for potential security vulnerabilities.
- **Physical Security**
  - ITD and NDUS use video surveillance and have restricted access to all offices and data center locations and require security badges which log physical access to restricted areas.



## NDUS - ITD Security Comparison - DIFFERENCES

- **Governance**
  - ITD has a documented Security Framework and a very mature Enterprise Architecture with established processes to support proactive security and threat mitigation.
  - NDUS has security policies and procedures in place without an established Enterprise Architecture structure.
- **Proactive Security Information and Event Management**
  - ITD manages a Security Information and Event Management system to correlate information and events from multiple systems.
  - NDUS uses extensive system and event logging but does not have a Security Information and Event Management System in place to proactively correlate the information.



## NDUS - ITD Security Comparison - DIFFERENCES

- **Security Staffing**

- ITD currently has 6 FTE's focused on IT security and risk management.
- NDUS currently has 2 FTE's focused on IT security and risk management.

- **Training**

- ITD requires regular security training for all ITD staff and state employees.
- NDUS is currently planning to implement required, regular security training for all staff.



## NDUS - ITD Security Comparison - NEXT STEPS

- Implementation of perimeter intrusion detection/prevention system on HE network
- Implementation of 2 factor authorization on NDUS critical systems
- Re-engineered desktop management and full disk encryption
- Re-engineered vulnerability scanning for improved proactive resolution of identified issues
- Updated Identity Management System for effective user management
- Implement mandatory security training for all NDUS employees



QUESTIONS?