

# **Governor's Cybersecurity Task Force**

**Monday, November 23, 2015  
Roughrider Room  
State Capitol Building**



# Agenda

## Topic

October Meeting Highlights - Lt. Gov. Drew Wrigley

NAIC Cybersecurity Overview - Adam Hamm, ND Insurance Commissioner

Current State of Cybersecurity Governance - ITD

Open Discussion:

Task Force Perspectives on Cybersecurity Governance

Closing Comments



# Meeting of the Governor's Cybersecurity Task Force on November 23, 2015

Adam Hamm, Commissioner  
North Dakota Insurance Department



# Overview

- ▶ Work of the NAIC's Cybersecurity Task Force
- ▶ Ongoing collaborative work with the federal government

# Insurance Industry Data Breaches

- ▶ Data breaches of 4 major insurance companies have been discovered so far in 2015
- ▶ The 4 insurance companies are Anthem, Premera, Care First and Excellus
- ▶ Over 100 million Americans have been impacted by these 4 breaches

# NAIC Cybersecurity Task Force

- ▶ NAIC established the Cybersecurity Task Force in late 2014
- ▶ Largest committee of the NAIC
- ▶ NAIC assigned me as Chair in January of 2015
- ▶ Responsibility of the Task Force to establish the insurance regulatory “rules of the road” in cybersecurity

# Guiding Principles

- ▶ “Flag in the ground” regarding the role of insurance regulators in cybersecurity
- ▶ Adopted by the NAIC Task Force in April
- ▶ Represents our overall cybersecurity strategy
- ▶ May be the type of document that our state task force wants to consider developing

# Consumer Bill of Rights

- ▶ Statement about what consumers can expect from insurers
- ▶ Information about consumer disclosures
- ▶ Information about services provided when a data breach occurs
- ▶ Adopted by the NAIC Task Force in October

# Data Collection on Cyber Insurance

- Cyber liability insurance market increasing in relevance as entities look for a measure of protection and risk transfer
- Developed a Cybersecurity Supplement to the Annual Financial Statement that's filed by P/C insurance companies each year:
  - Number of policies written
  - Premium and loss information
  - Market trends

# Information Sharing/Collaboration

- ▶ The Financial and Banking Information Infrastructure Committee (FBIIC)—N.D. represents all state insurance regulators on FBIIC
- ▶ The Cybersecurity Forum for Independent and Executive Branch Regulators (The Forum)—N.D. represents all state insurance regulators on The Forum





## National Governor's Association - Act and Adjust

- Establish a Governance Structure for Cybersecurity
- Conduct Risk Assessments and Allocate Resources Accordingly
- Implement Continuous Vulnerability Assessments
- Ensure Your State Complies With Current Security Methodologies and Business Disciplines in Cybersecurity
- Create a Culture of Risk Awareness



## North Dakota Cybersecurity Governance

- State Government
  - ITD Chief Information Officer - NDCC 54-59
- Statewide Critical Infrastructure and Key Resources
  - Department of Emergency Services - NDSLIC  
(ND State and Local Intelligence Center)
- Higher Education
  - NDUS Vice Chancellor for IT and Institutional Research
- K-12 Education
  - Educational Technology Council and EduTech



## ND Cybersecurity Governance - State Government

- ITD Chief Information Officer
  - Per NDCC 54-59-05.2 and 54-59-05.14 ITD has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets.
- CIO Executive Advisory Committees
  - State Information Technology Committee (SITAC)
    - NDCC 54-59-07
    - 18 Members - All 3 Branches of Government, Higher Education, 11 State Agencies and 2 Private Sector Members
  - Legislative Information Technology Committee
  - Governor's Cybersecurity Task Force



## ND Cybersecurity Governance - State Government

- ITD Operations - Deputy CIO
  - Security Division lead by a Chief Information Security Officer
  - Security roles and responsibilities in our Network Services, Computer Systems and Software Development divisions
- ITD Advisory Committees
  - IT Coordinators Council (ITCC)
    - All 3 Branches of Government - 13 core agencies
  - Enterprise Architecture - Security Architecture Team
    - 13 Security Related Standards
- Partnerships
  - Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - InfraGard
  - NASCIO and NASTD



North Dakota  
Information Technology Department

## ITD Cybersecurity Framework



State of North Dakota  
Information Technology Department  
Cybersecurity Framework  
April 4, 2014

Chief Information Officer

A handwritten signature in black ink that reads "Mike J. Ressler".

Mike J. Ressler



Deputy CIO/Director of ITD

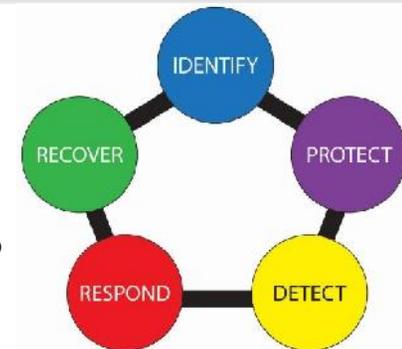
A handwritten signature in black ink that reads "Daniel E. Sipes".

Daniel E. Sipes



## ITD Cybersecurity Framework - Functions

- **Identify** - What do I need to protect?
  - **Protect** - What controls do I use?
  - **Detect** - How do I know I am being attacked?
  - **Respond** - What actions do I take?
  - **Recover** - How do I return to normal operations?
- Effective security encompasses the relationship between all five functions - it is a process, not a product.





## ITD Cybersecurity Framework - Functions

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Based on NIST Framework

- 5 Functions
- 22 Categories
- 18 Control Families
- 225 Controls
- 669 Control Enhancements



## Cybersecurity Framework Roles and Responsibilities

- Six Main Roles and Responsibilities
  - Senior Management (ITD and CIO Advisory Committees)
  - Information Security Management (ITD)
  - Information/Application Owner (State Agencies)
    - Agency Director
    - Agency IT Coordinator
    - Agency Security Officer
  - Technology Providers (ITD and/or Vendors)
  - Supporting Functions (Audit, Physical Security, DR)
  - Users (State Agencies and their Stakeholders)



## Cybersecurity Roles and Responsibilities

- ITD's Role (IS Security Management and Technology Provider)
  - Per NDCC 54-59-05.2 and 54-59-05.14 ITD has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets.
  - ITD is responsible for protecting the availability, integrity, and confidentiality of the state's information systems and the data stored in information systems that are managed by ITD.
  - ITD also directs the development of standards, policies and guidelines for enterprise security. This is done in collaboration with state agencies through the ITCC and Enterprise Architecture process.



## Cybersecurity Roles and Responsibilities

- Information/Application Owner (State Agencies)
  - ITD does not own most of the information residing in the data center. The information owner for most data is a state agency or political subdivision.
  - The information owner is responsible for being aware of the various applications and data they own.
  - The information owner is responsible for authorizing access privileges and ensuring regular reviews and updates to manage changes in risk profiles.



## Cybersecurity Roles and Responsibilities

- Agency Director
  - Agency Directors are responsible for information security in each agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise.
  - The director also is responsible for ensuring compliance with state enterprise security policies and with state and federal regulations.
  - Per NDCC 54-59-10 each agency must appoint an information technology coordinator to maintain a liaison with ITD. The agency director will often delegate their information security responsibilities to the agency information technology coordinator.



## Cybersecurity Roles and Responsibilities

- Agency IT Coordinator  
This role is assigned by the Agency Director and their security responsibilities include:
  - Submitting security requests
  - Reviewing access logs
  - Reviewing authorization reports
  - Serving as the main point of contact between ITD and the agency regarding security issues
- These duties are sometimes delegated to the Agency Security Officer.



## Cybersecurity Roles and Responsibilities

- Agency Security Officer
  - Agency Security Officers are responsible for communicating with ITD's Security Incident Response Team and coordinating agency actions in response to an information security incident.
  - In many agencies the Agency IT Coordinator fills this role.
- Agency User
  - Responsible for complying with the provisions of IT security policies and procedures.



## North Dakota Cybersecurity Governance



**Discussion on  
Governance  
and  
Roles and Responsibilities**



## Application Inventory and Risk Categorization



Agency	Name or acronym
Division	If applicable within your agency
Business Function	Short description such as Case Management, Unemployment Payments, etc.
Agency Contact	Primary application owner
System Short Name	If applicable; often an acronym
System Full Name	System title; without acronyms
Users	Internal (within agency), External (other agencies/partners), and/or Public
Data	Personally Identifiable Information (PII), Protected Health Information (PHI), Internal Use, and/or Public Use
Access	Internal via STAGEnet and/or external via the public internet
Authentication	None, NDGOV Active Directory, ND Login (LDAP), and/or Other
Developed By	ITD, Agency, and/or Other
Hosted By	ITD, Agency, and/or Other
Cost	Acquisition, Maintenance/Support, and Hosting



## North Dakota Cyber Disruption Response Strategy

- Focusing on Cybersecurity for Critical Infrastructure and Key Resources in the State of North Dakota.
- Specific goals are still under development but working goals are:
  - Improve Situational Awareness in the various sectors.
  - Create Plans for Cyber Threat Prevention, Mitigation, Response and Recovery
  - Train Staff and Conduct Exercises of Plans
  - Conduct Risk Assessments to Identify Vulnerabilities
- Coordinated by ITD and the Department of Emergency Services



# Closing Comments



**THANK YOU!!!**

## High Level Cybersecurity Relationships and Strategies - November 2015

