



# The STAGEnet Security Model

Peeling Away the Layers

March 17, 2015

NDSU Memorial Union

Rose Room



## NDSU 2015 Cyber Security Conference



# Art Bakke

Enterprise Information Security Administrator /  
Security Architect



## Goal



- To describe how security is strategically developed and implemented for STAGEnet enterprise network based on the needs of the various stakeholders.



## Agenda



- The Crown Jewels
- Roles and Responsibilities
- STAGEnet
- Cybersecurity Framework



# The Crown Jewels



### From Cradle



| Sex    | 1st | 2nd | 3rd | 4th | 5th | 6th | 7th | 8th | 9th | 10th | 11th | 12th |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|------|------|
| Male   |     |     |     |     |     |     |     |     |     |      |      |      |
| Female |     |     |     |     |     |     |     |     |     |      |      |      |

CONCORDS BY REGISTER

1st Period

2nd Period

3rd Period

4th Period

5th Period

6th Period

7th Period

8th Period

9th Period

10th Period

11th Period

12th Period

13th Period

14th Period

15th Period

16th Period

17th Period

18th Period

19th Period

20th Period

21st Period

22nd Period

23rd Period

24th Period

25th Period

26th Period

27th Period

28th Period

29th Period

30th Period

31st Period

32nd Period

33rd Period

34th Period

35th Period

36th Period

37th Period

38th Period

39th Period

40th Period

41st Period

42nd Period

43rd Period

44th Period

45th Period

46th Period

47th Period

48th Period

49th Period

50th Period

51st Period

52nd Period

53rd Period

54th Period

55th Period

56th Period

57th Period

58th Period

59th Period

60th Period

61st Period

62nd Period

63rd Period

64th Period

65th Period

66th Period

67th Period

68th Period

69th Period

70th Period

71st Period

72nd Period

73rd Period

74th Period

75th Period

76th Period

77th Period

78th Period

79th Period

80th Period

81st Period

82nd Period

83rd Period

84th Period

85th Period

86th Period

87th Period

88th Period

89th Period

90th Period

91st Period

92nd Period

93rd Period

94th Period

95th Period

96th Period

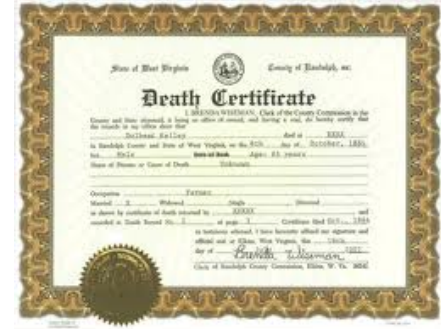
97th Period

98th Period

99th Period

100th Period

### To Grave



### And Beyond!





## ITD's Roles and Responsibilities



- 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 Enterprise Architecture process.
  - **Centralized Model**



## ITD Security Administrator Roles and Responsibilities



- Lead enterprise information security team; manage and provide oversight for information security projects and programs
- Develop security direction for ITD, State of North Dakota, political subdivisions & K-12 schools
- Provide guidance to meet technical & legal requirements for access to 1,700+ servers, 10,000+ endpoints for 100,000+ users



## What is STAGEnet?



### **STAGEnet**

- The North Dakota Statewide Technology Access for Government and Education network (STAGEnet) provides broadband connectivity, Internet access, video conferencing and other networking services to all state agencies, colleges and universities, local government, and K-12.





## What is STAGEnet? (continued)



- STAGEnet is governed as a partnership between government and education that consists of three committees\*, which aid in planning, prioritizing, approving standards, policies and procedures. Because of the varied nature and the variety of resources that use this network, security for it is built based on layers much like those of an onion.
  - \*Executive Committee (State CIO, NDUS CIO, K12 Director, ITD Network Services Director)
  - \*Management Committee (State, NDUS, ITD, IVN)
  - \*Technical Committee (State, NDUS, ITD, K12)



# 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



# Cybersecurity Framework



## Table of Contents

|   |            |
|---|------------|
| <b>1.0 Framework Introduction</b> .....                                       | <b>1</b>   |
| 1.1 Overview of the Framework .....   | 2          |
| 1.2 Risk Management and the Cybersecurity Framework .....                     | 2          |
| 1.3 Document Overview .....   | 3          |
| <b>2.0 Roles and Responsibilities</b> .....                                   | <b>4</b>   |
| 2.1 Senior Management .....   | 4          |
| 2.2 Computer Security Management .....  | 5          |
| 2.3 Program and Functional Managers/Application Owners .....                  | 5          |
| 2.4 Technology Providers .....  | 5          |
| 2.5 Supporting Functions .....  | 6          |
| 2.6 Users .....   | 7          |
| <b>3.0 Framework Basics</b> .....   | <b>8</b>   |
| 3.1 Framework Core .....  | 8          |
| <b>4.0 How to Use the Framework</b> .....                                     | <b>11</b>  |
| 4.1 Basic Overview of Cybersecurity Practices .....                           | 11         |
| 4.2 Establishing or Improving a System Security Plan .....                    | 11         |
| 4.3 Communicating Cybersecurity Requirements with Stakeholders .....          | 12         |
| 4.4 Identifying Opportunities for New or Revised Informative References ..... | 12         |
| <b>Appendix A: Framework Core</b> .....                                       | <b>A-1</b> |
| <b>Appendix B: North Dakota Century Code Related to Cybersecurity</b> .....   | <b>B-1</b> |
| <b>Appendix C: Glossary</b> .....   | <b>C-1</b> |
| <b>Appendix D: Acronyms</b> .....   | <b>D-1</b> |
| <b>Appendix E: Computer Security Incident Response Policy</b> .....           | <b>E-1</b> |
| <b>Appendix F: Remote Access Policy</b> .....                                 | <b>F-1</b> |



## Cybersecurity Framework



- Security Framework Roles and Responsibilities
  - ITD Executive and Information Security Management
    - CIO/Deputy CIO Responsibilities
    - Enterprise Security Administrator
    - ITD Virtual Security Team
  - Information/Application Owners
    - Agency Directors
    - Agency IT Coordinators
    - Agency Security Officers



## Cybersecurity Framework



- Security Framework Roles and Responsibilities
  - Technology Providers
    - ITD Architects
    - Project Managers
    - Developers
    - Network and System Administrators
  - Supporting Functions
    - Audit, Physical Security, Contingency Planning
    - Quality Assurance, Training, Procurement
    - Human Resources, Facilities
  - Users of Information and Systems



# Cybersecurity Framework Core



- Security Areas
  - Network Security
  - Host Security
  - Application Security
  - User Security

| 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                                 |
| PR                         | Protect  | PR.AC                      | Access Control                                  |
|                            |          | PR.AT                      | Awareness and Training                          |
|                            |          | PR.DS                      | Data Security                                   |
|                            |          | PR.IP                      | Information Protection Processes and Procedures |
|                            |          | PR.PT                      | Protective Technology                           |
| DE                         | Detect   | DE.AE                      | Anomalies and Events                            |
|                            |          | DE.CM                      | Security Continuous Monitoring                  |
|                            |          | DE.DP                      | Detection Processes                             |
| RS                         | Respond  | RS.CO                      | Communications                                  |
|                            |          | RS.AN                      | Analysis  |
|                            |          | RS.MI                      | Mitigation                                      |
|                            |          | RS.IM                      | Improvements                                    |
| RC                         | Recover  | RC.RP                      | Recovery Planning                               |
|                            |          | RC.IM                      | Improvements                                    |
|                            |          | RC.CO                      | Communications                                  |



# Cybersecurity Framework

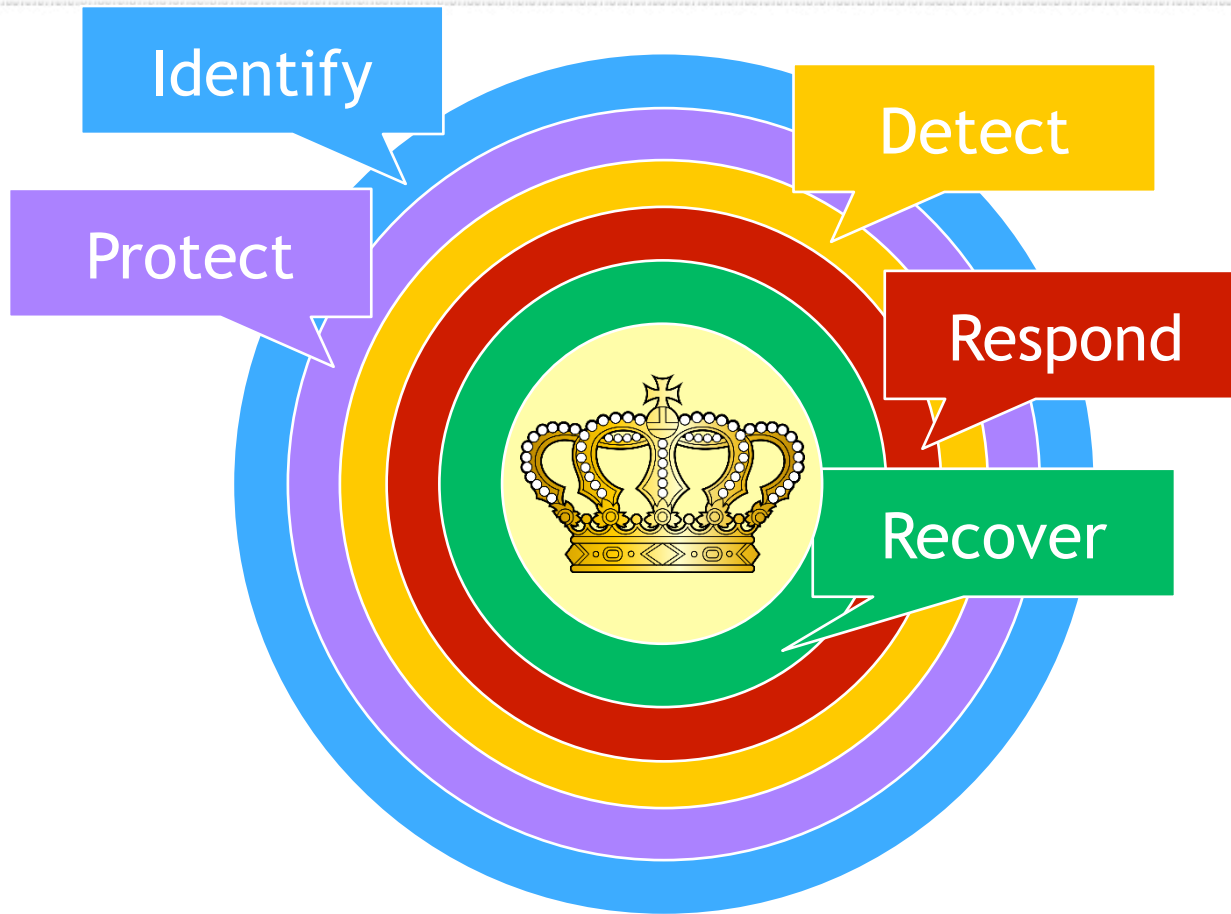


Appendix A – Framework Core

| Function        | Category  | Subcategory  | Policies   | Informative Resources   |
|-----------------|---|--|--|---|
| RESPOND<br>(RS) | <b>Response Planning (RP):</b><br>Response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events  | RS.PL-1: Response plan is implemented during or after an event.  | <ul style="list-style-type: none"> <li>ITD IR</li> </ul> | <ul style="list-style-type: none"> <li>ISA 99.02.01 4.3.4.5.1</li> <li>NIST SP 800-53 Rev. 4 CP-10, IR-4</li> <li>CCS CSC 18</li> </ul>                                 |
|                 | <b>Communications (CO):</b><br>Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies | RS.CO-1: Personnel know their roles and order of operations when a response is needed  | <ul style="list-style-type: none"> <li>ITD IR</li> </ul> | <ul style="list-style-type: none"> <li>ISO/IEC 27001 A.13.2.1</li> <li>ISA 99.02.01 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4</li> <li>NIST SP 800-53 Rev 4 CP-2, IR-8</li> </ul> |
|                 |   | RS.CO-2: Events are reported consistent with established criteria  | <ul style="list-style-type: none"> <li>ITD IR</li> </ul> | <ul style="list-style-type: none"> <li>ISO/IEC 27001 A.13.1.1, A.13.1.2</li> <li>ISA 99.02.01 4.3.4.5.5</li> <li>NIST SP 800-53 Rev 4 IR-6, IR-8</li> </ul>             |
|                 |   | RS.CO-3: Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties |  | ISO/IEC 27001 A.10  |
|                 |   | RS.CO-4: Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties  | <ul style="list-style-type: none"> <li>ITD IR</li> </ul> | <ul style="list-style-type: none"> <li>ISO/IEC 27001 A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2</li> <li>NIST SP 800-53 Rev. 4 CP-2, IR-8</li> </ul>                           |
|                 |   | RS.CO-5: Voluntary coordination occurs with external stakeholders (ex. business partners, information sharing and analysis centers, customers)                                   |  | NIST SP 800-53 Rev. 4 PM-15, SI-5]  |



## Cybersecurity Functions - The basis for our Framework

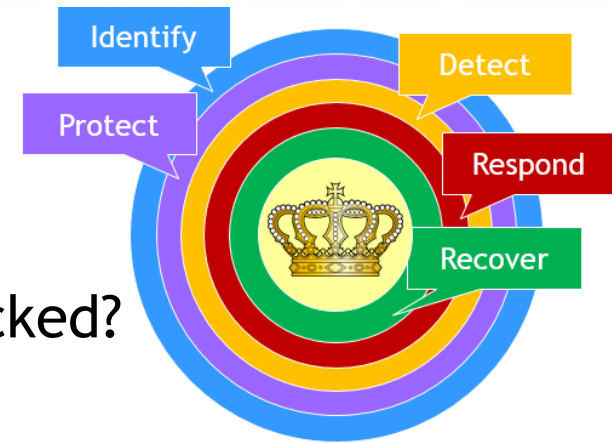






## Cybersecurity Functions - The basis for our Framework

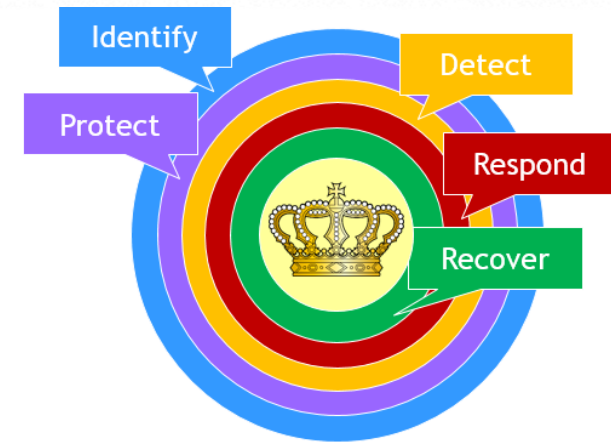
- **Identify** - What do I need to protect?
  - **Protect** - What controls do I use?
  - **Detect** - How do I know I am being attacked?
  - **Respond** - What actions do I take?
  - **Recover** - How do I return to normal operations?
- Effective security encompasses the relationship between all five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





## Cybersecurity Principles

- Security by Design
- Defense in Depth
- Compartmentalize
- Utilize Control Points (Choke) Points
- Fail Securely
- Secure the Weakest Link

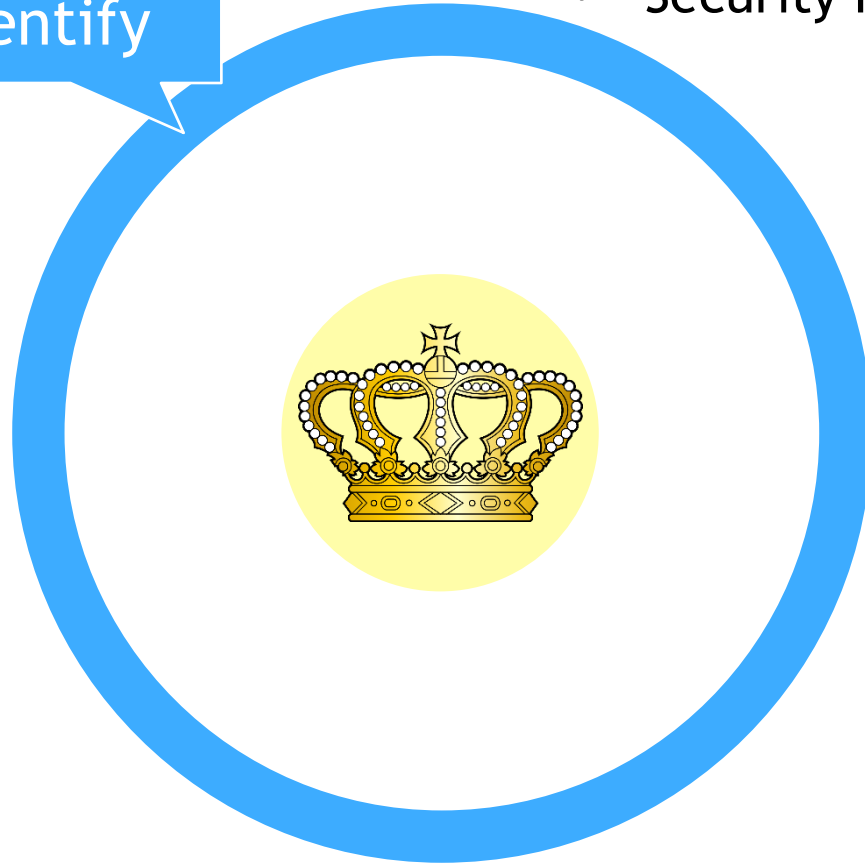




## What Do I Need to Protect?



Identify



- Security Frameworks

- Audits/Risk Assessments

- Data Classification



## What controls do I use?



- Encryption
- Virtual Private Networks (VPN)
- Advanced Firewalls & Intrusion Prevention Systems (IPS)

Protect



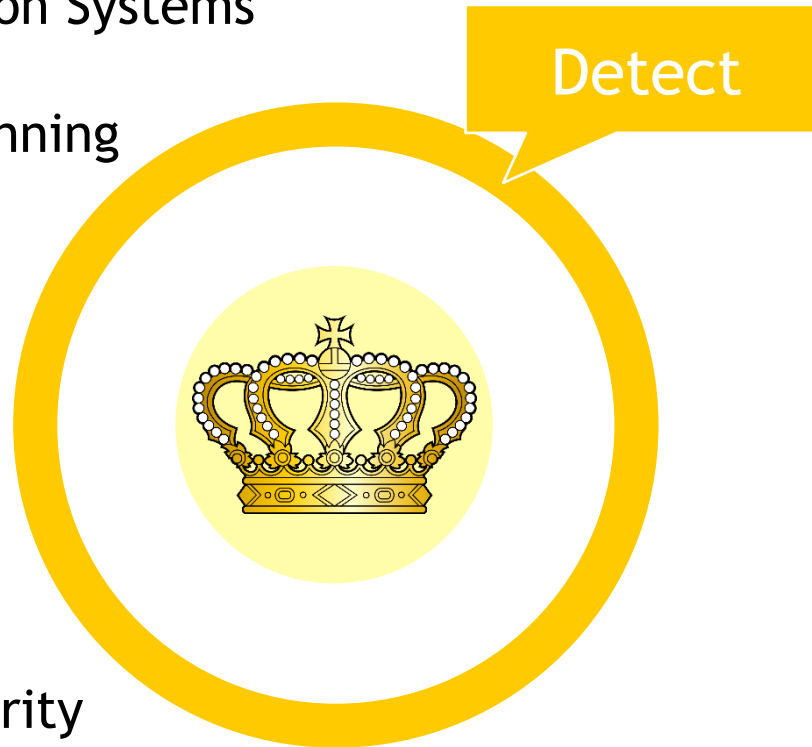
- Physical Security
- Awareness & Training
- Identity & Access Management



## How do I know I am being attacked?



- Intrusion Detection Systems (IDS)
- Vulnerability Scanning



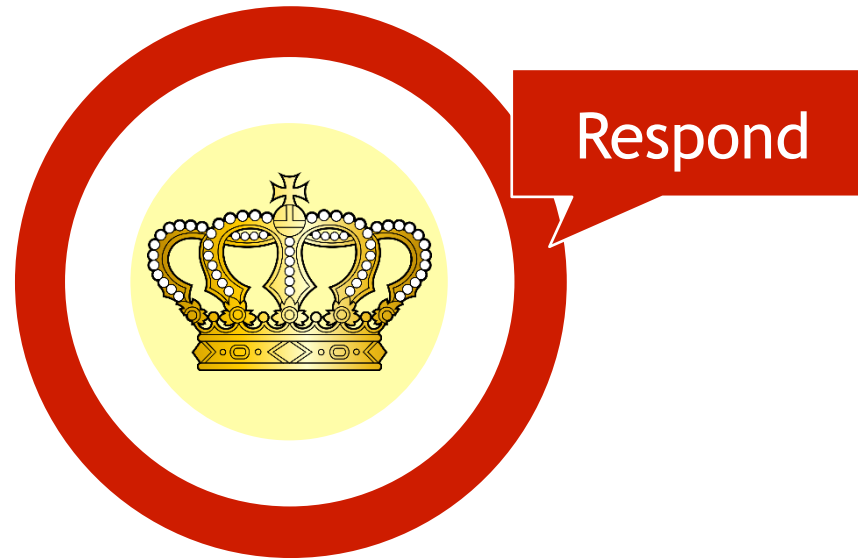
- Audit Logs - Security Information and Event Management (SIEM) Systems



## What actions do I take?



- Security Incident Response Team and processes
- Cybersecurity Forensics
- Proactive Vulnerability Management





## How do I return to normal operations?



- Contingency Planning
- Data Backups and High Availability Systems
- Secondary Data Centers





## Conclusion

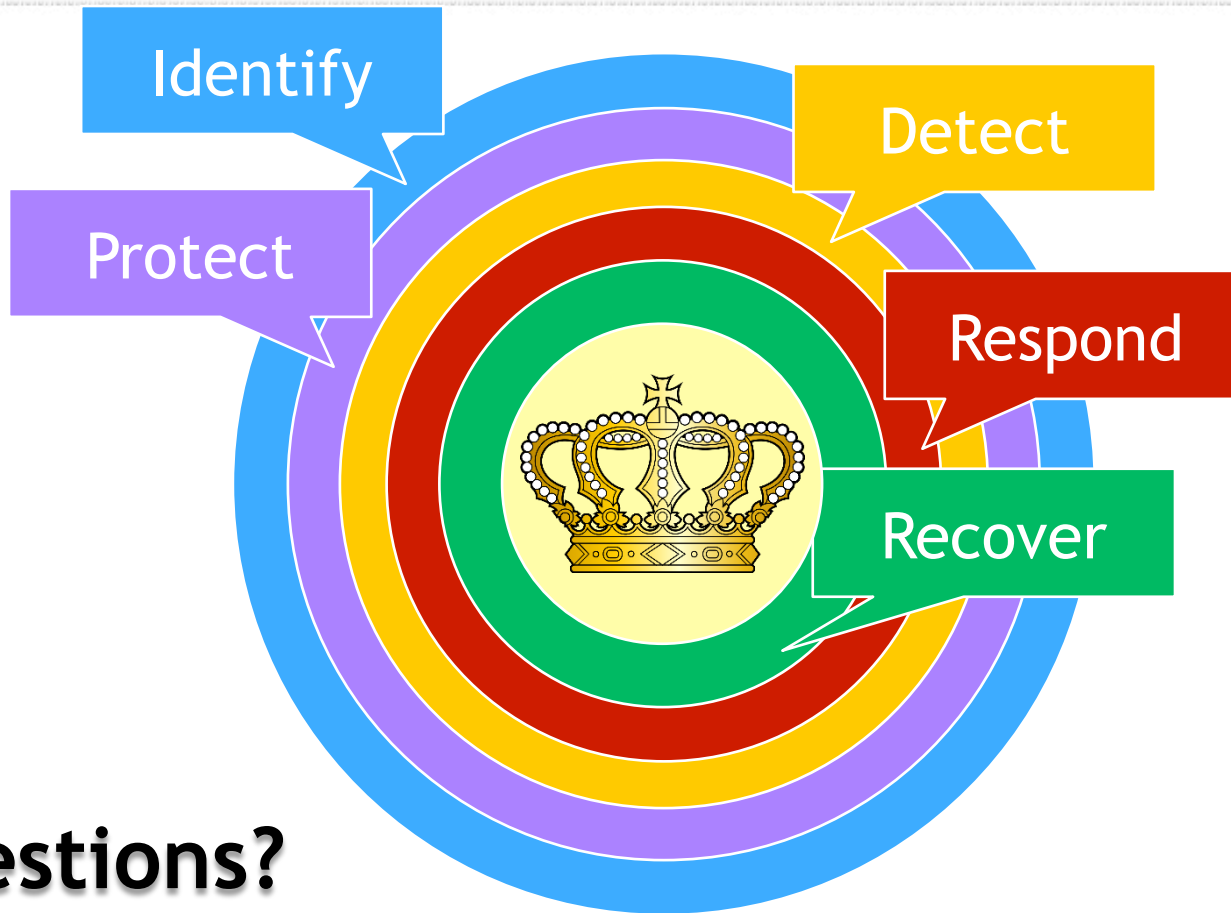


- The Crown Jewels
- Roles and Responsibilities
- STAGEnet
- Cybersecurity Framework





## Cybersecurity Functions - The basis for our Framework



Questions?



# Thank you!

Art Bakke

Enterprise Information Security Administrator /

Security Architect

State of North Dakota

[ambakke@nd.gov](mailto:ambakke@nd.gov)