IT Oversight Meeting
Cybersecurity Update

Maria Thompson
Chief Risk Officer

March 5, 2020

Enterprise Security and Risk Management Office (ESRMO)

Mission

Provides leadership in the development, delivery and maintenance of an information security and risk management program that safeguards the state's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss. The ESRMO supports a comprehensive statewide program that encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprise business continuity management. The ESRMO works with executive branch agencies to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements. Working with state agencies, federal and local governments, citizens and private sector businesses, ESRMO helps to manage risk to support secure and sustainable information technology services to meet the needs of our citizens

Why is Cybersecurity Important?

Key component of any risk management strategy

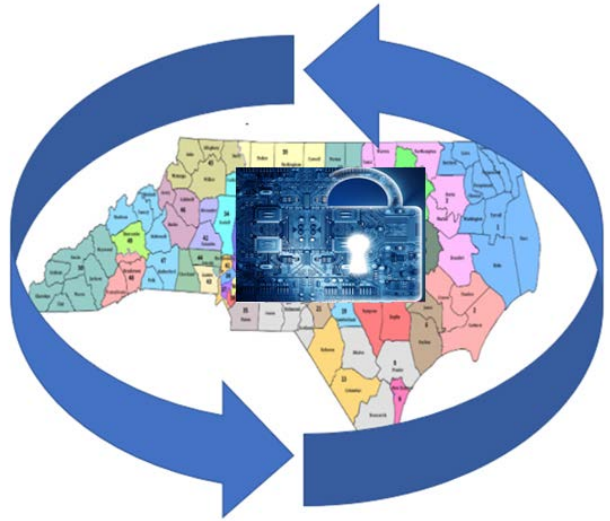
- State and local government IT struggle with obtaining and building it into business requirements
- Shadow IT activities are prevalent throughout the state
- State agencies, local government and academia are resource constrained – lack of manpower
    - Local county networks host critical services for the state:
        - Critical infrastructure, e.g. elections, water, power etc.
        - Life and safety services, e.g. 911, health, public safety
- Current decentralized cyber practices, ad hoc cyber budgeting and lack of accountability for cyber risks leads to inconsistent cyber approach and poor risk management
    - Limited network visibility
    - Legacy systems with no maintenance or patch support
    - Ineffective identity, credential and access management
    - Slow incident response capabilities

Strategic Objectives

Key Initiatives
• Develop, implement and fund a statewide cyber incident response capability to support secure citizen engagements • Reduce the risks to the state's critical infrastructure by collaborating with local government • Advance the state's cyber workforce through education and collaboration with K-12 and higher education • Protect and secure statewide government and academic networks • Assess, trend and evaluate emerging cyber risks to the state • Support federal and state partners in combatting cybercrime targeting citizens and small businesses • Establish a statewide privacy program to address growing concerns on data management practices

Whole-of-State Cyber Approach

Eliminating all risks is virtually impossible— unifying cyber, managing risks and building resilience will be the key to a more secure state!



- BitSight monitoring of local county infrastructure
- Pilot program for continuous monitoring of local county network traffic
- Developed of Statewide Significant Cyber Incident Plan
- Established statewide information sharing under HB 217
- Cyber incident response and training support utilizing National Guard Defensive Cyber Operations team and local IT Strike teams

NC Reported Ransomware Attacks

Date	Affected Entity	Ransomware /Malware
Feb. 2016	Durham	Unknown
Dec. 2017	Mecklenburg County	LockCrypt
Feb. 2018	Davidson County	SamSam
May 2018	Pasquotank County	Scarab
Oct. 2018	Onslow County Water and Sewer	Ryuk
Nov. 2018	City of Durham	Unknown
Mar. 2019	Orange County (hit 3 times in 6 yrs)	Ryuk
Mar. 2019	Pasquotank-Camden EMS	Unknown
Mar. 2019	Robeson County	Ryuk
Apr. 2019	City of Greenville	RobinHood
Jul. 2019	Richmond Community College	Ryuk
Aug. 2019	Lincoln County Sheriffs Office/911 (X2)	DopplePaymer
Sep. 2019	NC Commission	DopplePaymer
Oct. 2019	NC State Bar	Neshta (dropper)
Oct. 2019	Columbus County School System (x17)	Ryuk
Oct. 2019	ABC Board (x21)	Sodinokibi
Dec. 2019	EBCI	Sodinokibi (Insider Threat)
Jan. 2020	Duplin	Ryuk

Govt Supporting Govt – NC National Guard

NCNG - Cyber Assessment and Assist Team

UNCLASSIFIED//FOR OFFICIAL USE ONLY
CLOSE HOLD//DO NOT DISTRIBUTE

20-001 Statewide Cyber Assessment

- DIT Funded - 10 Soldier Cyber Assessment and Assist Team
- Prioritize Assessing 40 Tier 1 Counties until 01JUL2020

Focus:

Security Program Review, Environmental Factors, Technical Review Policies, Cyber Hygiene, Configuration Baselines, Patch and Vulnerability Management

Concept of Operations:

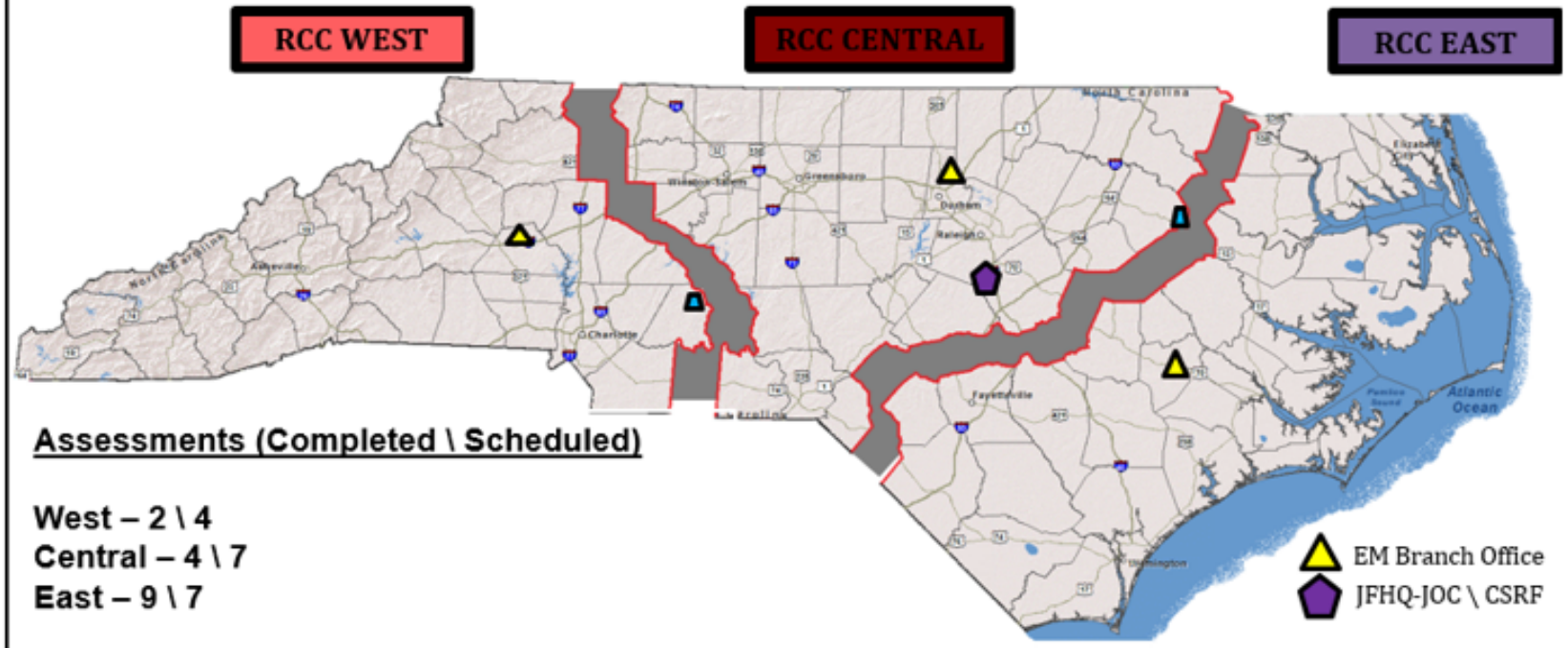
- Scope: Schedule, SOW, Rules For the Use of Cyber
- Assess: Hands on Onsite Assessment, Executive and Technical Reports
- Train: Remediation Training

End State:

Allow the counties to "See Themselves" from a cyber risk perspective

"Train" the counties in remediation techniques from assessment findings

Understand the total threat landscape across NC counties



Assessments (Completed \ Scheduled)

West – 2 \ 4
Central – 4 \ 7
East – 9 \ 7

*** Schedule completely full through MAY**

Category I Finding:

Definition: allow primary security protections to be bypassed if compromised

Per location: [redacted] CAT I findings
Total: [redacted] CAT I findings

Bottom Line: Exploits developed and available

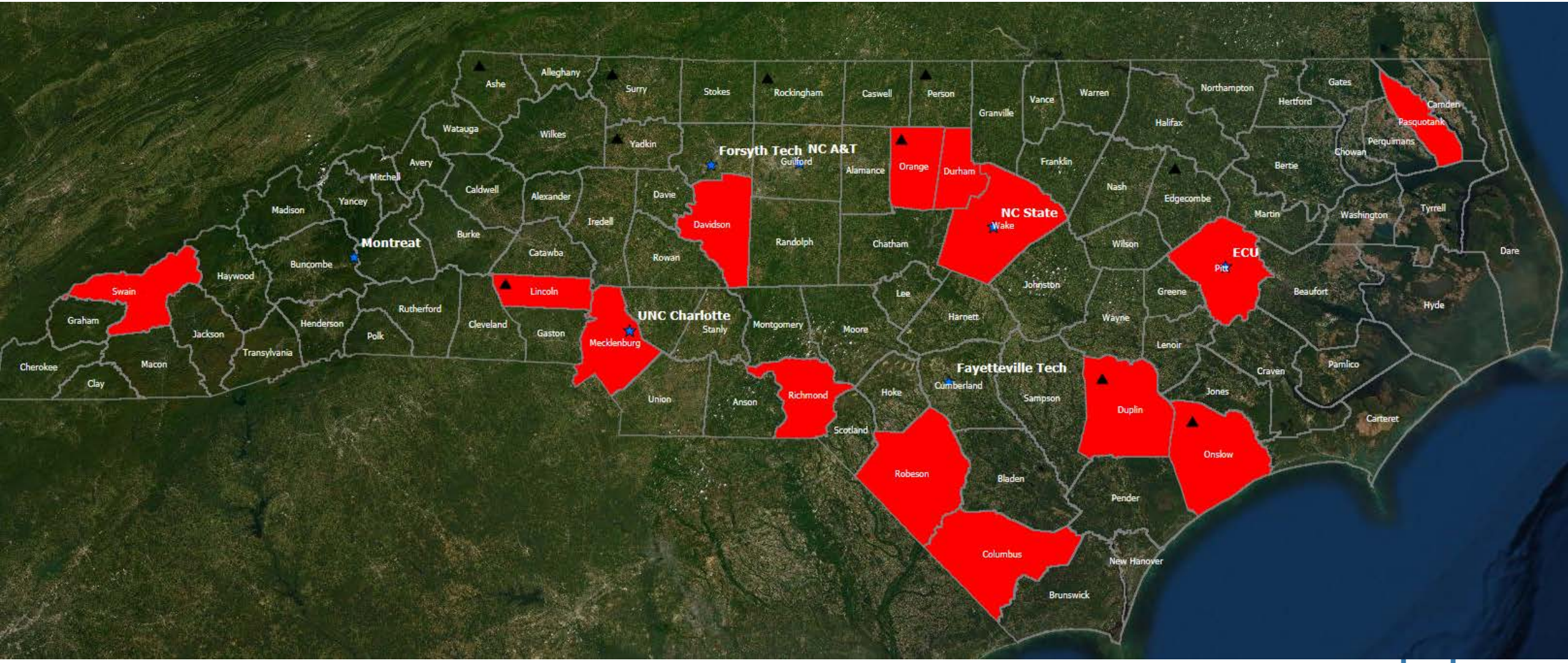
Category II Finding:

Definition: potential to lead to unauthorized system access

Per location: [redacted] CAT II findings
Total [redacted] CAT II findings

Bottom Line: Exploit development required

Govt Supporting Govt – NC National Guard



Continuous Monitoring & Annual Compliance Reporting

- N.C.G.S. 143B-1376 requires the State CIO to annually assess the ability of each agency and their contracted vendors to comply with the current enterprise-wide set of security standards. The information gathered is used to build out the State IT Plan. These assessments include, at a minimum:
  1. Rate of compliance with the enterprise-wide security standards
  2. Estimate of cost to implement deficient security measures
  3. Assessment of Security Organization
     - Security practices
     - Security industry standards
     - Network security architecture
     - Current expenditures of state funds for IT security

- ESRMO has developed a Continuous Monitoring Plan that requires all agencies to complete an annual risk and security assessment and have ongoing processes in place to assess the current posture of the environment.
  - All critical systems must obtain a third-party assessment within a **3-year cycle**. In the off-years, agencies conduct an annual self assessment..

Let’s Connect!

@NCDIT
@BroadbandIO
@ncicenter

NC Department of Information Technology

NCDIT

NC DIT

@NCDIT

it.nc.gov