Monthly Cybersecurity Newsletter

March 2018 Issue

NC DIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

New Policies for Statewide Security!

The State Chief Information Officer (State CIO) has approved a new set of statewide information technology policies that are designed to enhance the security posture of the State. The new policies are based on the National Institute of Standards and Technology (NIST) 800-53 database of security controls. One of the reasons the policies were transitioned to the NIST Risk Management Framework (RMF) was to better align the State's security controls with Federal standards and reduce auditing overhead. These new policies were developed with the assistance of subject matter experts and peer reviewed by agency representatives using NIST 800-53 controls as the framework.

The policies are the foundation for security and privacy in the state of North Carolina. These policies provide State agencies with a *baseline* for managing information security and making risk based decisions. They also provide requirements for protecting the security and integrity of citizens' personal and confidential information, and they regulate the use of the Internet and other information technology resources by state employees. The policies apply to all executive branch agencies, their agents or designees that are subject to Article 15 of N.C.G.S. §143B. Local governments, local education agencies (LEAs), community colleges, and constituent institutions of the University of North Carolina (UNC) are encouraged to use these policies to the extent the law allows. The policies align to the following seventeen NIST controls:

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance		

The new statewide security policies may be found at https://it.nc.gov/statewide-resources/policies. In addition, a crosswalk will be available that shows the relationships between the new policy requirements and the previous Statewide Information Security Manual as well as other standards and frameworks.

GDPR is Coming Soon…but What is It?

There is a new global security regulation on the horizon. It is the European General Data Protection Regulation (GDPR) and it will impact the processing of all personal data on European Union (EU) residents. The GDPR is the EU's latest mechanism to mitigate privacy risk where the impact on an individual is highest. GDPR stresses the importance of a data subject's rights, the manner in which data breaches are handled, and general control over personal data. It goes into effect on ***May 25, 2018***.

If an organization has an establishment in the European Union, this new regulation applies. But the effect goes beyond territorial boundaries of the EU alone. If an organization offers services or goods to the EU, the GDPR applies as well. The same goes for organizations that, regardless of their own establishment, are monitoring an individual's behavior in the EU. This includes, for example, tracking an individual online to create a profile, or even to determine or predict the individual's preferences. The initial approach toward GDPR compliance includes the following steps, which are also appropriate for helping any organization have a more secure posture:

- ***Raise Awareness***: Make sure key personnel are aware of privacy and security requirements.
- ***Assess Information***: Document what personal data is being held, where it came from, and to whom it is shared.
- ***Document Legal Basis***: Identify the legal basis for storing and processing personal data.
- ***Communicate Privacy Information***: Review privacy notices and plan for necessary changes.
- ***Review Data Protection Procedures***: Review procedures, including how to delete data, how to provide data electronically, and how to respond to data access requests.
- ***Review Consent Management***: Review how to seek, record and manage consent to data and whether any changes to current procedures are necessary.
- ***Update Data Breach Procedures***: Make sure the right procedures are in place to detect, report and investigate data breaches, and update those procedures as necessary.
- ***Designate a Data Protection Officer***: Designate someone to take responsibility for data protection compliance and assess where this role will be in the organization.
- ***Support Continous Improvement***: A continuous risk assessment, as well as planning and prioritizing security improvement, are just as important as selecting the appropriate security controls for the current operation. *Assess and adapt as the context changes!*

Will organizations be ready for GDPR? Experts say many will not. It is estimated that less than 50% of all organizations impacted by GDPR will fully comply with it by the time it goes into effect. Data breaches to an organization can lead to significant damage to its finances and its reputation. Before 2020, there will be a multimillion Euro regulatory sanction on organizations that are not compliant to GDPR. Companies that fail to comply with the GDPR can be fined up to 4% of their global annual revenue or 20 million Euros, whichever figure is highest. More importantly, media coverage following such a finding can cause substantial damage to a company's reputation. For more information, visit https://www.eugdpr.org/key-changes.html.

Don't forget the other **monthly newsletters** that are available to you! The following are the various cybersecurity newsletters the ESRMO distributes each month. We hope you find them beneficial.

- **SECURITYsense Newsletter:** A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. **Note:** *You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource*.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access), Extranet, or other public access network is strictly prohibited.

- **Security Tips Newsletter:** A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is on ***Staying Safe from Tax Scams***.

https://www.cisecurity.org/resources/newsletter

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Top Tips to Securely Using Social Media.***

https://www.sans.org/security-awareness-training/ouch-newsletter

---

Did you know that The SANS Institute also provides *free* awareness **videos** and **webcasts**? The SANS Video of the Month may be accessed at https://securingthehuman.sans.org/resources/votm.

Also, The SANS Institute offers free webcasts on a variety of topics that may be accessed at https://www.sans.org/webcasts/upcoming.

Upcoming SANS Webcasts:

4/3/2018 – *Apple's latest file system - is APFS a blessing or a curse to digital investigators?*

4/10/2018 – *Digital Trust in a Perimeterless World*

4/11/2018 – *Practical Approach to Detecting and Preventing Web Application Attacks over HTTP/2*

4/18/2018 – *One Detect to Win: Tactical Application Detection*

5/1/2018 – *BreakingPoint: A Multi-Function Tool for Application and Security Testing*

** Access to these webcasts as well as a list of many others may be found via the link above!*

Hurricane Virtual Tabletop Exercise!

The Federal Emergency Management Agency's (FEMA) Emergency Management Institute (EMI) Virtual Tabletop Exercise (VTTX) program will offer three sessions of a hurricane scenario on **April 24, 25 and 26**. Each month, EMI conducts a VTTX series using a Video Teleconference (VTC) platform to reach community-based training audiences around the country by providing a virtual forum for interactive disaster training. The VTTX is designed for a group of 10 or more representatives from state, local, tribal, and territorial emergency management communities of practice. It provides a unique opportunity for responders across the Nation to simultaneously participate in a hazard-specific, facilitated discussion. Additional information is available at https://training.fema.gov/programs/emivttx.aspx.

The VTTX occurs 12pm–4 pm ET. To participate in this event, send an email to Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Also, send a courtesy copy email to the Integrated Emergency Management Branch at fema-emi-iemb@fema.dhs.gov or call 301-447-1381. The application deadline is **April 6, 2018**. Content is the same each day, and participants would attend only one session.

~~~

Also, don't forget the EMI e-Forums! These are 1-hour, moderated, webinar discussion forums that provide an opportunity for the EMI and the emergency management community to discuss matters of interest on national preparedness training. These exchange of ideas and best practices are free of charge and available to anyone who wishes to participate. The forums are scheduled on **Wednesdays in March** from 3:00pm– 4:00pm EST.

- Login link: https://fema.connectsolutions.com/emieforums
- Conference call-in: 800-320-4330, PIN 107622

Check out the following resources…

- Department of Information Technology (DIT) Site: https://it.nc.gov/
- Cybersecurity and Risk Management Site: http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management
- Cybersecurity Awareness Page: https://it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness
- State of NC Cybersecurity Situation Report: https://it.nc.gov/cybersecurity-situation-report

---

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.
~~~