2024 NASCIO NOMINATION

Cross-Boundary Collaboration and Partnerships

How Can We Help?

Supporting Local Governments Through Joint Cybersecurity Efforts

Initiated: February 2020
Completed: July 2024

Contact: James Weaver
North Carolina State Chief Information Officer
Secretary, N.C. Department of Information Technology
919-809-3845
james.weaver@nc.gov

NCDIT
NORTH CAROLINA
DEPARTMENT OF
INFORMATION
TECHNOLOGY

Executive Summary

Governments are prime targets for bad actors, who are continually evolving their skillsets and making their attack tactics increasingly sophisticated. It is not a question of if, but when, they will become susceptible to an incident.

In many cases, the targets are local government entities that may not have the personnel, funding or resources to adequately prepare for and defend against cyberthreats, and their vulnerabilities can threaten the security of the entire state.

In response to these challenges, North Carolina Gov. Roy Cooper issued Executive Order 254 in March 2022 formalizing the Joint Cybersecurity Task Force (JCTF), which brings together the N.C. Department of Information Technology (NCDIT), the N.C. National Guard, N.C. Emergency Management and the N.C. Local Government Information Systems Association (NCLGISA) IT Strike Team. Along with other local, state and federal agencies, the JCTF provides technical guidance and support upon request to government and educational entities faced with cyberthreats.

The executive order's intent was to increase the task force's visibility among not only local governments, but also critical infrastructure and key resource partners such as hospitals, airports and utilities. The executive order encourages these entities to work with the task force to coordinate effective cyber defensive efforts that can help limit the impacts of a cybersecurity incident. Another goal of Executive Order 254 was to increase communication and build trust and relationships among entities to ensure a strong response to cyber incidents.

Through North Carolina's whole-of-state approach to cybersecurity and the engagement of the JCTF, NCDIT and its partners have been able to provide support across the entire state through shared defensive capabilities, training and tabletop exercises, relationship building and boots on the ground response efforts.

Separately, NCDIT is pursuing a number of initiatives to bolster local government cybersecurity efforts and safeguard government assets across North Carolina.

Idea

NCDIT's Enterprise Security and Risk Management Office (ESRMO) takes a whole-of-state approach to cybersecurity management, partnering with federal, state and local entities to gain and share insights that help inform cybersecurity policy and strategy statewide.

The ESRMO works with the state's IT Strategy Board and its Cybersecurity and Privacy committee, which prioritizes cyber needs across the state. The committee and the IT Strategy Board help promote the importance of cybersecurity investment and ensure that state decision-makers are aware of the funding requirements for a robust cybersecurity presence. The statewide strategy is established based on a gap analysis that considers feedback and recommendations from partners.

The success of the whole-of-state approach also hinges on building and maintaining strong relationships with local government organizations for regular engagement and communication on their cyber initiatives and needs. In partnering with local governments, NCDIT has recognized the importance of asking “how can we help?” and providing access to tools, training, expertise, manpower and other resources that can strengthen and quicken cyber response and protect the state from threats.

Cybersecurity is a team effort that requires all entities to work transparently with each other. To that end, Executive Order 254, which established the JCTF that brings together federal, state and local security experts, is focused on fostering communication, collaboration and coordination to break down silos that prevent or slow down cybersecurity efforts.

State, county and municipal government entities in North Carolina are required by statute to report significant cybersecurity incidents, such as ransomware attacks, to NCDIT. The same statute also encourages private entities to report them.

Bolstering these statutory efforts, Executive Order 254 strongly encourages critical infrastructure and key resources in both the public and private sectors to take three main actions to facilitate a more accurate holistic understanding of the state’s cyber risk landscape beyond government:

- Report cybersecurity incidents, such as ransomware attacks, to the JCTF in order to request assistance.
- Allow the task force to come alongside reporting entities during such incidents, even if the entity has cyber insurance and/or their own cyber resources.
- Report public-facing IP addresses so the task force can be proactive and assist in identifying and responding to cybersecurity vulnerabilities.

When a significant cyber incident is reported by state or local government or an educational entity like a school or university, the task force convenes to assess the situation, coordinate any incident response and discuss other resource support and technical assistance needed to help keep incidents from happening again.

Implementation

JCTF Efforts

When a compromise occurs and a request for assistance is made, the JCTF team provides forensics within the environment and attempts to identify what occurred all the way back to initial access. The team then helps with recovery processes and recommendations, from simple, cost-free ways to improve security posture all the way to next generation security tools that are offered at the enterprise level.

The JCTF is also engaged in proactive measures that help protect local government agencies from cyber threats including:

N.C. 911 Tabletop Exercises and Cybersecurity Remediation Funding

The N.C. 911 Board, a unit of NCDIT, is focused on increasing cybersecurity awareness for the public safety answering points (PSAPs) it funds across the state. In 2023, the board hosted a series of four cybersecurity exercises for managers and staff at PSAPs and the IT staff who support them. The exercises, led by the N.C. 911 Board, U.S. Cybersecurity and Infrastructure Security Agency and JCTF, covered cybersecurity best practices, roles, responsibilities and training for PSAPs.

In the exercises, representatives from three North Carolina PSAPs described their real-world experiences surrounding compromise incidents and the lessons learned from their responses. Trainers then led the participants through a discussion of their own experiences, preparations and opportunities for improvements in cybersecurity, and PSAP staff shared cybersecurity best practices.

The board has also provided vulnerability assessments to PSAPs and offers them funding for cybersecurity remediation. Six cybersecurity remediation initiative proposals have been approved this year, totaling more than $485,000. In addition, the N.C. 911 Board has hosted several cybersecurity planning sessions this year in conjunction with the JCTF and CISA to provide a forum where the PSAPs can create and implement incident response plans and procedures leveraging the knowledge of the state partners.

National Guard Assessments

The N.C. National Guard performs proactive security assessments utilizing National Institute of Standards and Technology (NIST) standards in conjunction with Department of Defense Security Technical Implementation Guidelines. These assessments fulfill annual requirements and also identify potential security, configuration or network design deficiencies that may adversely impact the confidentiality, availability or integrity of agency networks, devices and services.

Information collection techniques used by the assessment team include interviews with agency personnel, automated network discovery and scanning tools, open-source information gathering, obtaining of technical configuration information for a sample of key network infrastructure devices, examination of network documentation and inspection of network equipment including physical layer connectivity.

NCDIT Efforts

In addition to its involvement in the JCTF, NCDIT is undertaking a number of initiatives to support local governments' cybersecurity efforts and partner with them to prevent and respond to cyberthreats:

Centralized Purchasing and Funding of Cybersecurity Tools

NCDIT has prioritized central funding for a number of cybersecurity tools, starting with the implementation of Tanium as an endpoint detection and response tool. This project began in 2018, and many of the department's optimized agencies adopted the tool as early as 2019.

From 2022 to 2024, NCDIT successfully deployed the client to additional agencies including the state departments of Agriculture, Environmental Quality, Health and Human Services and Public Safety.

NCDIT secured funding in North Carolina's state budget for fiscal year 2024 to centrally fund Cloudflare, a web application firewall that provides edge protection for web applications and services, and CrowdStrike, which provides next generation endpoint protection for all executive branch agencies, for two years. NCDIT's goal is to secure recurring funding for these important tools to ensure key security capabilities are readily available at no cost to these agencies, eliminating a deterrent to implementation.

By providing enterprise security at a statewide level, NCDIT can obtain bulk discount rates and pass those savings on to other state and local entities who may not otherwise be able to afford the service. Another benefit of this approach is the centralized visibility and consistency it provides. Commonality in tools allows the state to operate as a centralized security operations center (SOC), helping speed up response and giving an improved picture of the state's overall cybersecurity landscape.

Cybersecurity Pilot Program

With $2.5 million in non-recurring funds appropriated for fiscal year 2020-2021, NCDIT established a pilot program to determine the feasibility of providing future cybersecurity services for local governments in economically distressed counties throughout the state. The goal of the program is to develop a partnership with a trusted third-party managed security services provider to conduct monitoring and management of cybersecurity functions within the supported entity's networks and devices.

In April 2022, NCDIT issued a request for proposals to solicit responses from managed security service providers for the cybersecurity pilot. The contract was then awarded to AT&T on March 7, 2023, with a term of one year and the option to extend for two additional one-year periods.

Two local governments – Lee and Nash – are participating in the pilot to ascertain the benefits, costs and long-term feasibility of an expanded program. The core security services being piloted include SOCaaS, End Point Detection and Response, and a Managed Vulnerability Program. The pilot has yielded data and metrics that have enabled its clients to prioritize and address potential gaps.

State and Local Cybersecurity Grant Program

North Carolina is receiving approximately $10.8 million in federal grant funding through the FY23 State and Local Cybersecurity Grant Program (SLCGP). North Carolina Emergency Management is charged with managing this grant for the state. NCDIT is responsible for providing programmatic and technical support.

The SLCGP allows the U.S. Department of Homeland Security to make targeted cybersecurity investments in state, local and territorial government agencies. The goal of the program is to help states, local governments, rural areas, tribes and territories address cybersecurity risks and cybersecurity threats to information systems.

The program requires a 20 percent non-federal cost share, or match, raising the total amount of funding to approximately $13.5 million. NCEM will provide the entire 20% non-federal cost share for the FY23 SLCGP. Required non-federal cost shares may be passed on to individual subrecipients if the state receives an SLCGP award in FY24 or any future years.

Impact

The JCTF has responded to 92 incidents since calendar year 2019, in addition to cyberthreats that have been thwarted through proactive engagement before having an impact on the state. This includes 16 incident responses in calendar year 2022 and 15 incident responses in calendar year 2023 on behalf of state agencies, county and local governments, universities and community colleges, and K-12 school systems.

Following the success of the JCTF's efforts, many states are emulating the partnerships that have been established as they work to mature their own cybersecurity programs.

NCDIT has also seen tremendous success in its implementation of Cloudflare and CrowdStrike. There are currently 95 state agency root domains being protected within Cloudflare with over 400 DNS records held under those root domains across 20 agency accounts. Application developers and owners are provided training, resources and support from NCDIT. This ensures that applications can be added to the platform and managed by the teams working within the applications.

For CrowdStrike, NCDIT deployed more than 60,000 clients across the state over the past two years, including nearly 37,000 in just a few days. This deployment vastly improves the security posture across the executive branch agencies and allows NCDIT's ESRMO to have global insight into rising cybersecurity threats that may be targeting various state agencies.

The rapid adoption of Cloudflare and CrowdStrike, in addition to the support of the federated tenancy model, allows individual agencies as well as the ESRMO to quickly identify threats to the state from endpoint devices, cloud workloads and public-facing web pages.

Recently, due to these improvements and better inter-agency and partner collaboration, NCDIT has been able to respond to several cybersecurity incidents so rapidly that quality evidence suggests threat actors were unable to steal data through exfiltration methods and were unable to complete intended ransomware encryption activities. This rapid response, facilitated by the whole-of-state, quality cybersecurity tools, and strong partnerships, resulted in a much quicker clean up, recovery and return to service for victim entities that would have otherwise not been possible in typical incident response cases.

Next Steps

NCDIT will be working with the General Assembly in the upcoming biennial budget process to establish a fund that will cover the costs for a two-year period to help cyber victimized Tier 1 counties reach a specific level of cyber hygiene. At the conclusion of the two-year period, the county will assume the operational costs.

In addition, the ESRMO and the Statewide IT Procurement Office, both part of NCDIT, have worked together to streamline the procurement process for cybersecurity solutions, which previously consisted of multiple contracts. These cybersecurity software, products and services have been consolidated into a single, comprehensive contract that will better serve the needs of state and local government agencies, public schools, community colleges and the member campuses of the University of North Carolina system. It is a mandatory Statewide Term Contract for the use of executive state agencies and may also be used as an optional Convenience Contract by non-state agencies as permitted by law.

This approach enhances the efficiency and effectiveness of acquiring robust cybersecurity solutions to ensure that the state's digital infrastructure is protected. It establishes a single, flexible and comprehensive portfolio of cybersecurity solutions that can meet the evolving procurement needs of the state and allows for the selection of individual cybersecurity products and services to align with specific agency requirements.

To ensure the contract remains current and inclusive of the latest cybersecurity advancements, it will be periodically reopened at the state’s discretion for the consideration of new vendors and the expansion of offerings by existing vendors. The term for the RFP is one year, however, the state retains the option to extend the agreement for two additional one-year periods.

The Statewide IT Procurement Office anticipates that the solicitation for the new Cybersecurity State Contract will be publicly posted for bid by the end of May. Bid awards for each cybersecurity category will be determined by the ESRMO.