NATIONAL GOVERNORS ASSOCIATION

M E M O R A N D U M

April 28, 2020

To: Governors' Offices
From: Bill McBride, Executive Director
Re: COVID-19 and Cybersecurity

State cybersecurity concerns – critical for governors under normal circumstances – have only intensified during the COVID-19 pandemic. Malicious cyber actors have a history of exploiting the confusion and fear surrounding crises,[1] which the current pandemic offers on an unprecedented scale. State agencies, critical infrastructure sectors, and the general public are experiencing waves of COVID-themed malicious cyber activity. The mass transition to remote work environments is a challenge for state networks while increasing their cyber vulnerability, providing threat actors even more opportunity. The stakes riding on states' abilities to prevent and protect its systems, staff, and entities within the state from cyberattacks is immense. A successful cyberattack on state networks or critical infrastructure, especially healthcare facilities, would cripple its ability to respond to and recover from COVID-19.

This memo provides:

- Actions for Governors Looking to Bolster State Cybersecurity
- An Overview of the Threat Landscape Facing States:
  - Increased Cyber Activity on State and Local Infrastructure;
  - Telework Vulnerabilities;
  - Cybercrime Concerns for Citizens; and
  - Mis & Disinformation Campaigns.

In addition to the recommendations below, NGA strongly encourages states to adhere to the cybersecurity best practices recommended by NGA and national cybersecurity experts, including using a whole-of-government approach to cybersecurity, updating and familiarizing incident response and cyber disruption plans, and messaging and practicing proper cyber hygiene.[2]

Actions for Governors to Bolster State Cybersecurity

- **Invest in cybersecurity.** With the shift to telework, state cybersecurity requires additional attention and investment for threat prevention and risk mitigation strategies. Talk with your state chief information officer (CIO) and chief information security officer (CISO) to determine top cybersecurity spending needs for state information technology infrastructure based on individualized risk assessments. Talk with your homeland security advisor to ensure investments are in line with the statewide homeland security strategy. To ease the costs of securing and modernizing IT infrastructure, NGA recommends that states leverage federally funded grant programs, including future stimulus bills. (Due to the COVID-19 crisis, NGA has requested that Congress authorize

[1] https://statescoop.com/natural-disasters-bring-cyberthreats-small-and-large/
[2] https://www.nga.org/bestpractices/divisions/hsps/statecyber/

and fully fund a dedicated cybersecurity program to help states, territories and localities implement innovative and effective cybersecurity practices.[3])

- **Raise awareness of the potential for increased cyber threats in times of crisis, both within state government and with the general public.** Malicious cybersecurity actors – from nation state actors to criminal organizations – are using focus on the disaster to their advantage. Governors should leverage their platform to address the public safety concerns due to COVID-related cyber threats, advance a culture of cybersecurity awareness and support for state cybersecurity experts, and promote trusted sources of information to counter mis- and disinformation campaigns.
    - Governors should work with IT and Public Safety offices to issue public guidance and advisories. States are also issuing cyber alerts, telework guidance, and consumer protection information on agency websites. For example, the **Delaware** Department of Technology and Information, the **Iowa** Department of Public Safety, **North Carolina** Department of Information Technology, **Texas** Department of Information Services and **Washington** Office of Cybersecurity released cyber advisories and toolkits related to COVID-19.[4] The states offer guidance and alerts on current fraud schemes (e.g., Washington regularly posts screenshots of phishing emails[5]), cybersecurity tips and best practices for consumers, remote work and virtual meetings, available federal and state resources, and information for victims on how to report cybercrime.
- **Ensure your information technology agency implements best practices for cyber hygiene and cybersecurity with increased teleworking, including:[6]**
    - Where required, state personnel should log into state networks through a virtual private network (VPN) that is fully patched and use multi-factor authentication to reduce vulnerabilities. [7]
    - Agencies should review bring-your-own device (BYOD) policies to account for increased attacks on employee-owned devices.
    - IT professionals should fully configure and install security software for any issuance of new technology for remote workers.
    - State cybersecurity experts should continually monitor state networks for vulnerabilities and prioritize the mitigation of those vulnerabilities based on severity, risk of exploitation, and asset criticality. This includes monitoring and reducing "shadow tools" by proactively providing state-owned devices to staff.
    - Work with agencies to ensure they protect and back up data to accelerate the recovery process.

---

[3] https://www.nga.org/policy-communications/letters-nga/coalition-letter-cybersecurity-it-covid19/

[4] Read the Delaware advisory here, the Iowa advisory here, the North Carolina advisory here, Texas advisory here and the Washington advisory here.

[5] https://cybersecurity.wa.gov/news

[6] CISA's guidance on risk management is available at https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf. Additional recommendations include implementing micro-segmentation strategies for state networks and deploying endpoint detection and response (EDR) technology on remote users' laptops. Please see CISA's Interim Telework Guidance for more information, available at https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf.

[7] For more information on VPN use and alternative approaches, including the "zero trust" model, see https://www.beyondcorp.com/

- Require that virtual meetings should be secured via password to prevent unauthorized access.
- Enhance employee cybersecurity education and training programs. Continue the practices that an alert workforce would be doing in a workplace, including encouraging employees to identify and report suspicious emails and messages, connect to secure Wi-Fi and avoid clicking on unknown links. Communicate to staff expectations for how they will receive information via internal emails (e.g., in the body of the email rather than through zip folders or links) and that they should never expect to receive internal emails requesting personal identifiable information or login credentials.[8]

- **Incorporate security-by-design standards into any new IT project and public-facing websites.** As states look to use technology to respond to the pandemic, security controls are critical for any mitigation effort that stores user data. Security should be factored into the architecture/design of any platform deployed by states. Likewise, states should secure public-facing websites, including those created to enhance constituent services or communicate public information on COVID-19 response efforts.
- **Understand the important role that information technology plays in continuity of operations (COOP) and continuity of government (CoG), as a cyber disruption could impact your state's ability to respond and recover from COVID-19.** State agencies should be familiar with their cyber incident response/statewide cyber disruption response plans.[9]
- **Consider deploying the National Guard to support cybersecurity response missions.**
  - Responding to Governor Hogan's state emergency declaration for the state of **Maryland**, the National Guard, Military Department, and Department of Information Technology established a joint cybersecurity taskforce for COVID-19 response.[10]
- **Support the healthcare and public health sector's cybersecurity,** including public health agencies, health care facilities and hospitals, as the sector has increasingly become a target of ransomware and other cyber attacks. While much of this sector is non-governmental, governors can encourage the sharing of cyber threat information between government, private sector, and critical infrastructure entities, specifically through participation in an Information Sharing & Analysis Organization (ISAO) or Information Sharing & Analysis Center (ISAC). Governors and their advisors can also direct those organizations' IT staff towards available cybersecurity resources, including low- or no-cost risk assessments, such as the no-cost Vulnerability Scanning service provided by DHS's Cybersecurity and Infrastructure Security Agency (CISA).[11]
  - The California State Operations Center (SOC) established the COVID-19 CA-ESF18 (Cybersecurity) Task Force, comprised of federal and state partners to monitor, alert, and share cyber threat information, and respond to cyber incidents

[8] Recommendation by Ryan Kalember, Executive Vice President, Proofpoint, during NGA State Coronavirus Action Network (SCAN) Call on April 16, 2020. For more information, see https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/03/12/cybercriminals-seek-profit-in-coronavirus

[9] For additional information about state incident response and cyber disruption response plans, see https://www.nga.org/center/publications/hsps-publications/state-cyber-disruption-response-plans/

[10] https://news.maryland.gov/ng/2020/04/04/mdng-serves-real-virtual-communities-in-covid-19-response/

[11] CISA offers this service to state and local agencies as well as private sector organizations within your states – to include healthcare and public health organizations. Further information is available at: https://www.cisa.gov/cybersecurity-assessments.https://www.cisa.gov/cybersecurity-assessments

related to COVID-19 and the healthcare sector. The Task Force established a team to scan agency networks, including public health agencies, to detect vulnerabilities and offer remediation recommendations.[12]

- **Bolster cybercrime enforcement, particularly for COVID-related online scams or frauds,** and support state cybercrime enforcement investigative agencies, particularly those participating in a task force. Provide guidance and support for victims of cybercrime.[13]
    - **Virginia** and **West Virginia** launched task forces dedicated to combatting rising fraud schemes and cybercrime around the public health emergency. The task forces are joint federal-state initiatives in conjunction with the FBI, the states' assistant U.S. attorneys, and representatives from the states' law enforcement and Attorney General's offices.[14]

Threat Landscape

Increased Cyber Activity on State and Local Infrastructure:

Threat actors, ranging from anonymous cybercriminals to advanced persistent threat (APT) groups, have exploited the current crisis to launch attacks against government institutions, critical infrastructure, corporations, and the public. Since January, there have been over a million malicious COVID-themed messages, URLs, and attachments stemming from hundreds of campaigns preying upon the distraction, confusion, and fear caused by COVID-19.[15] Themes for these lures typically relate to government aid, procurement of personal protective equipment (PPE), and access to testing. While some APT and groups linked to nation states are motivated through espionage, the majority of the campaigns seek financial gain.

Common vehicles for COVID-related lures are phishing scams and business email compromise (BEC) campaigns that seek to either deploy malware, including ransomware, or access user data and credentials.[16] Phishing attempts may manifest as seemingly authentic email or text messages sent by trusted sources – ranging from organizations like the World Health Organization (WHO), Center for Disease Control (CDC), and the White House to a doctor's office or an interoffice email – that lure the user to open contaminated links or attachments.[17] Types of malicious activity include:

- *Malware and ransomware*: Malware and ransomware attacks have increased sharply during the COVID pandemic as malicious actors find that organizations, particularly state agencies or healthcare organizations, may be more likely to pay ransoms given the urgency to keep critical systems and services operational.[18]

---

[12] https://www.caloes.ca.gov/LegislativeExternalAffairsSite/Documents/COVID19%20Key%20Messages.pdf

[13] For additional information and resources for cybercrime victims, see https://fraudsupport.org/

[14] Read more about Virginia's Coronavirus Task Force here and West Virginia's Coronavirus Fraud Task Force here.

[15] https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat

[16] https://www.us-cert.gov/ncas/alerts/aa20-099a

[17] *Ibid*.

[18] E.g., the Champaign-Urbana Public Health District in Illinois was hit by ransomware in March 2020. Under pressure to restore operations, the district met the hackers' demands. Its cyber insurance paid over $300,000 in ransom and the district paid its $10,000 deductible. See https://www.govtech.com/security/Illinois-Health-System-Hacked-Amid-Coronavirus-Response.html; Additionally, an urgent care facility in Texas was hit with ransomware, seizing sensitive patient data while

- *Credential theft*: Some phishing attempts may prompt a user to enter account passwords, thereby allowing access to accounts, emails, and sensitive information to be used for either financial gain or to advance additional phishing attacks.
- *Business email compromise*: In BEC attacks, victims receive an email from a trusted associate that alters standard payment practices, e.g., a request that funds be sent to a new account.[19] BEC campaigns are targeting state and local governments looking to procure PPE and other supplies necessary for COVID-19 response.
- *Watering hole attacks*: In these attacks, threat actors hijack legitimate websites in order to distribute malware or steal users' credentials.[20]

Telework Vulnerabilities:

Public sector entities and critical infrastructure sectors are prime targets for cyber threat actors given their role in COVID-19 response and recovery efforts. The shift to remote work has heightened their cyber vulnerability as state IT infrastructure becomes overburdened and the potential use of personal devices and home networks create new gateways for malicious activity.

- *Increased cybersecurity risk with remote infrastructure:* Employees' homes, networks, and potential use of personal devices are now the frontlines of organizations' cyber defenses.[21] It is essential that state IT agencies ensure that employees are equipped to handle the cybersecurity risks associated with telework environments. Virtual private networks and other remote work infrastructure may have been rapidly deployed without the latest patch or update.[22] Phishing and BEC campaigns looking to deploy malware or steal credentials or funds prey upon distracted employees burdened by the mental toll of the pandemic – efforts to educate, train and raise employees' cyber awareness should be prioritized. Threat actors are also targeting organizations' reliance on virtual conferencing software: there has been a significant rise in phishing websites containing fake domain names – e.g., "ZO0M.us.com" – and security breaches where unauthorized users can eavesdrop, hijack, and otherwise disrupt virtual meetings, e.g., "zoombombing."[23]

---

affecting its digital equipment and interrupting daily operations. See https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/. For additional information on the increase in ransomware during the COVID-19 pandemic, see https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/

[19] https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

[20] Many of these campaigns have occurred in foreign countries, but in March 2020, two websites operated by San Francisco International Airport (SFO) were targeted. For more information, see https://sfoconnect.com/about/news/notice-data-breach-march-2020

[21] The shift to remote work poses security concerns for the private sector as well. See https://www.tenable.com/blog/how-to-secure-a-work-from-home-organization-insights-from-a-cso

[22] For additional information on VPN security, see https://www.us-cert.gov/ncas/alerts/aa20-073a and https://www.us-cert.gov/ncas/alerts/aa20-107a

[23] From January 1, 2020 to March 30, 2020, Checkpoint found that more than 1,700 new domains were registered and 25% were registered in the last week of March. Out of these registered domains, 4% have been found to contain suspicious characteristics. For more information on the rise in fake domain names, see: *https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/*; For more information on video teleconferencing hijacking, see: *https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic*

- *Strained network capabilities*: The rapid shift to telework has tested states' capacity to provide secure and effective services. Demand for state-issued devices, e.g., laptops, tablets, smart phones, has surged where use of personal devices is prohibited. Support staff may be overburdened with the increase in service disruptions and bandwidth issues stemming from collaborative software to fully focus on network security.[24] Likewise, state CIOs and CISOs, homeland security advisors, emergency managers, and guardsmen are under significant time and resource pressures dealing with the state's response to the pandemic and may have less capacity than under normal circumstances, further reducing real-time response capability and placing more importance on pre-pandemic response plans.[25]

Cybercrime Concerns for Citizens:

In addition to attacks against the public sector and critical infrastructure, private citizens are subject to numerous COVID-related fraud schemes. The amount of incidents reported has surged – ranging from online extortion schemes[26] to COVID-related phishing scams, luring targets with references to testing kits, PPE procurement, and federal relief checks.[27] Other lures, through charity and romance scams relying on fraud and social engineering, seek to exploit the loneliness, isolation and generosity wrought by the pandemic and social distancing for financial gain.[28] Cyber criminals are also taking advantage of the rise in online shopping, as digital skimmers swipe payment information from retail sites.[29] In 2020, there have been over 22,000 consumer complaints and $16.6 million lost to COVID-related fraud schemes.[30]

Mis & Disinformation Campaigns:

The public has also been subject to mis- and disinformation campaigns, many operated by nation-state actors – primarily China, Iran and Russia – looking to exploit the confusion caused by COVID-19 and sow further discord.[31] While attribution is challenging, news outlets have pointed to China as the source of the unsuccessful March distributed denial of service (DDoS) attack on the U.S. Department of Health and Human Services' website, which would have prevented access to public information on the pandemic response.[32] U.S. intelligence agencies' assessments indicate that Chinese operatives helped amplify rumors of an imminent national quarantine that were spread via a SMS disinformation campaign in March.[33] An internal European Union report warns of a Russian-backed disinformation campaign against the West to spread panic and

[24] https://www.nascio.org/wp-content/uploads/2020/04/NASCIO_COVID19_PlanningforStateCIOs_v2.pdf
[25] *Ibid*.
[26] https://www.ic3.gov/media/2020/200420.aspx
[27] https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection
[28] https://fraudsupport.org/wp-content/uploads/2020/04/FraudSupport.org-COVID-19-Scams.pdf; For additional information see https://cybercrimesupport.org/the-epidemic-of-romance-fraud/
[29] https://www.wired.com/story/magecart-credit-card-skimmers-coronavirus-pandemic/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202
[30] https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints-041920.pdf
[31] https://www.njhomelandsecurity.gov/analysis/iranian-russian-and-chinese-media-drive-covid-19-disinformation-campaign
[32] https://apnews.com/7edbc93627b1040a422f2d07f50d4cda
[33] https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html

confusion. [34] Additionally, the media has reported that Iranian-linked accounts have spread propaganda on social media platforms.[35] Experts have attributed mis- and disinformation campaigns not only to foreign actors, but domestic hate groups using social media platforms to spread lies and fear as well.[36] Influence operations may also emerge in the discourse surrounding reopening the economy.

For questions or concerns related to the contents of this memo, please contact NGA staff:

- *Maggie Brunner (mbrunner@nga.org; 202.624.5364)*
- *John Guerriero (jguerriero@nga.org; 202.624.5372)*

[34] An internal EU document states that "a significant disinformation campaign by Russian state media and pro-Kremlin outlets regarding COVID-19 is ongoing." See: "https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F

[35] https://www.forbes.com/sites/thomasbrewster/2020/04/15/iran-linked-group-caught-spreading-covid-19-disinformation-on-facebook-and-instagram/#164a73201f21

[36] https://www.splcenter.org/hatewatch/2020/04/17/hate-groups-and-racist-pundits-spew-covid-19-misinformation-social-media-despite-companies