

# NGA Cybersecurity Newsletter

September 29, 2020

Contact: John Guerriero ([jguerriero@nga.org](mailto:jguerriero@nga.org))  
202-624-5372

---

## Resource Center Announcements

October is National Cybersecurity Awareness Month, and this year's theme is "Do Your Part. #BeCyberSmart." Read more about the NCSAM theme, schedule of events, and resources from the Cybersecurity Infrastructure Security Agency (CISA) [here](#).

Please feel free to send any news and information on your state's plans and upcoming events to John Guerriero [here](#).

### **2020 National Cybersecurity Awareness Month Sample Governor Proclamations Released**

CISA and the MS-ISAC recently distributed the [NCSAM 2020 Proclamation](#) to every Governor and CISO's office across the country to increase local level cyber outreach and awareness. Please feel free to share the proclamation with your jurisdictions for their sign-on.

### **Upcoming NGA Webinars**




#### **October 26: SLTT Indicators of Compromise Automation Pilot**

Please join NGA on **October 26<sup>th</sup> from 3:00pm - 4:00pm ET** for the next Resource Center for State Cybersecurity webinar. We will highlight Arizona's participation in the Johns Hopkins University Applied Physics Laboratory pilot program that looks to share information in near real-time and leverage automation to prevent and respond to cyber-attacks. Our speakers from Arizona will discuss the state's application of Security Orchestration, Automation and Response (SOAR) program and share their experiences on how it helped shore up cyber defenses by reducing response time.

Please register for the webinar [here](#) and reach out to Khristal Thomas [here](#) with any questions.

### **Previous NGA Webinars**

- *Countering Election Mis- and Disinformation Campaigns* (September 22<sup>nd</sup>)
  - Slides are [here](#) and a recording is [here](#)

- The New Jersey Office of Homeland Security and Preparedness's Disinformation hub is [here](#).
- The Defending Digital Democracy Project (D3P) released its Election Influence Operations Playbook ([link](#)). The D3P team also released an Election Data Set – a living document collecting the different election regulations across the country ([link](#)). Also mentioned during the discussion was the D3P Elections Battle Staff Playbook ([link](#)).
- *On the Cyber Frontlines: The Role of the National Guard in Defending States and Local Governments* (webinar co-hosted with the National Association of Attorneys General and National Association of State Chief Information Officers – September 10<sup>th</sup>)
  - A recording is [here](#).
- *Ransomware Prevention Tactics for State and Local Government* (August 31<sup>st</sup>)
  - Slides are  [here](#) and a recording is [here](#)
  - Rapid7's [four-part e-book](#) on building an incident response plan
- *Election Cybersecurity with CIS & EI-ISAC* (August 26<sup>th</sup>)
  - Slides are  [here](#) and a recording is  [here](#)

### **NGA Launches Project with DOD on States' Role in National Defense**

NGA recently announced a two-year partnership with the Department of Defense Office of Economic Adjustment (OEA) to help governors and states work more closely with the defense sector, promote military resiliency and better realize more economic value from defense assets. Through a series of seven reports and workshops in 2020 and 2021, NGA and OEA will provide policy analysis and guidance on how state and territorial leaders can enhance their role in national defense while realizing the economic benefits of a vibrant, resilient defense sector.

NGA will continue to distribute updates and information on upcoming project opportunities, and feel free to read more about the project [here](#) or reach out to John Guerriero for more information [here](#).

### **NGA Request for Information:**

1. How is your state looking to expand and diversify its public sector cybersecurity workforce? Has your state looked at implementing public sector cybersecurity apprenticeship programs?
2. How has your state involved local jurisdictions in incident response planning? What does outreach look like? How has your state received information on local response plans and capabilities?

3. How is your state leveraging the National Guard in preparation for the upcoming election? Will it be deployed to provide cybersecurity support? If deployed in a non-cyber capacity, what roles will it fill?
4. How is your state agency coordinating with your state's election official to promote election cybersecurity? How is your state planning to address disinformation campaigns and public messaging strategies promoting a safe and secure election season? Please feel free to reach out John Guerriero [here](#) with any additional questions or technical assistance requests you have regarding election cybersecurity and resilience.

Please reach out to John Guerriero [here](#) on the above requests.

---

## Cybersecurity Resources

### Election Security Resources

#### CISA Election Resources

In partnership with the Election Assistance Commission, CISA's National Risk Management Center developed and released an assessment tool to support state and local election officials understand their risks and how to prioritize mitigation. Access the risk profile tool [here](#).

CISA also released an insight on strategies to counter email-based attacks on election-related entities. The guide offers recommendations for political parties and campaigns as well as other organizations on best practices to secure email systems. Read the insight [here](#).

See more of CISA's election security resources [here](#).

#### MITRE Releases 6 Steps to a Safe, Trusted Election

The MITRE Corporation released a technical paper outlining six recommended steps for state officials to take to help promote public trust in the election process. The recommendations include fighting election misinformation and setting public expectations for an election season, not an election night. Read the paper [here](#).

#### NGA Supports #TrustedInfo2020

NGA joins the National Association of Secretaries of State (NASS) in supporting [#TrustedInfo2020](#). The [bipartisan education effort](#) is aimed at promoting state and local election officials as the trusted sources of election information. [#TrustedInfo2020](#) aims to reduce the misinformation and disinformation surrounding elections by directing voters directly to election officials' websites and social media pages. NGA joins a host of other organizations in supporting NASS in this effort.

### **New Jersey Releases Supplemental Threat Assessment**

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) released its 2020-2021 Supplemental Threat Assessment, detailing how the national threat landscape is influenced by COVID-19, civil unrest, foreign disinformation campaigns, the upcoming election and other events. Read more about the assessment [here](#).

### **NIST Develops Method to Support Employee Phishing Training**

The National Institute of Standards and Technology (NIST) recently released a report on its Phish Scale tool that helps employers better train employees on avoiding phishing scams. The tool analyzes click rates and user feedback and applies a rating methodology that helps explain why employee click rates on phishing emails may be high or low. Read more about the tool [here](#).

### **Building the Federal Cyber Workforce**

The Cyberspace Solarium Commission released its third white paper, this one focusing on growing a stronger federal cyber workforce. The paper lays out five key elements for a federal strategy, including recruitment, development and retention. Read the paper [here](#).

### **Registration Opens for Girls Go CyberStart**

The [Girls Go CyberStart](#) program is available in 2020. Interested states should contact Alan Paller from the SANS Institute [here](#) for more information. NGA can provide governors' offices with additional information on this program – gubernatorial statements and announcements on the program have historically had a significant impact on student participation.

### **National Cybersecurity Career Awareness Week Call for Commitments**

November 9-14, 2020 marks National Cybersecurity Career Awareness Week, which looks to educate and engage students of all ages, educators, parents, and employers on the value of careers in cybersecurity. The National Initiative for Cybersecurity Education (NICE) released a call for commitments for those looking to participate in the week's activities. Learn more about National Cybersecurity Career Awareness Week [here](#).

### **Registration Opens for Cybersecurity Symposium for Smart Cities 2020**

Sponsored by the NIST, this symposium will look to connect government officials, small business and industry leaders, and nonprofits on strategies and innovative practices for supporting smart cities and communities. The event will take place from October 14-16 and you can register [here](#).

---

## Cybersecurity News

### **Ransomware Attack on Tyler Technologies**

After software provider Tyler Technologies was hit by a ransomware attack, customers have reported discoveries of suspicious logins and unauthorized remote access tools on their networks. Read more about the attack [here](#) and the company's statement [here](#).

### **Texas A&M Cybersecurity Apprenticeship Program Unveiled**

Texas A&M University, in partnership with the Cybersecurity Youth Apprenticeship Initiative (CYAI), launched a cybersecurity apprenticeship program that gives A&M students paid job experience working to defend the university networks as well as those of Texas state agencies, cities, and counties. The CYAI is funded through the U.S. Department of Labor. Read more about the program [here](#).

### **Disinformation Campaigns Remain Major Election Threat**

With the general election a month away, federal, state, and local officials are [working](#) to guard against disinformation campaigns, including holding tabletop exercises and launching digital advertising campaigns.

The FBI and CISA issued a public service announcement on the potential for disinformation around the election results, especially with the longer reporting timeframe expected due to the increased use of mail-in ballots. Read the announcement and its recommendations [here](#).

The agencies also released an announcement warning against attempts to cast doubt on legitimacy of the election, particularly those spreading false claims of hacked voter information. Read the announcement [here](#).

Likewise, in a testimony before the House Homeland Security Committee, FBI Director Chris Wray noted significant efforts by Russian actors to influence the 2020 election, while also noting the agency has not observed any foreign attacks on U.S. voter registration databases. Read more [here](#).

### **K-12 Cybersecurity a Major Issue Amidst Pandemic & Virtual Learning**

With the start of the school year and continued virtual learning, schools across the country are seeing an increased threat from cyber attacks. Tightened budgets have resulted in less money to spend on cybersecurity and dependence on virtual platforms has made school districts a ripe target for cyber criminals looking to disrupt operations or profit off ransomware. School districts (and all SLTT government organizations) looking for increased cybersecurity awareness and advisories can join the MS-ISAC for free. Read more about MS-ISAC membership [here](#) and recent K-12 cybersecurity news [here](#), [here](#) and [here](#).

### **NGA Government Relations Updates**

### **GAO Report Highlights Need for Central Cyber Leadership Role**

The U.S. Government Accountability Office (GAO) recently released a report on the need to define a central cybersecurity leadership role to coordinate government efforts and to hold federal agencies accountable. The report offers recommendations for executive action as well as a request for Congress to consider legislation designating a leadership position in the White House with the authority to implement and encourage action supporting national cybersecurity. Read more about the report [here](#).

### **House to Vote on State and Local Cybersecurity Improvement Act**

The House is set to vote this week on [H.R. 5823](#), the State and Local Cybersecurity Improvement Act, which would create a state and local cybersecurity grant program. Read more [here](#).

---

## NGA Resource Center for State Cybersecurity Partners

- Amazon Web Services
- American Electric Power
- AT&T
- CompTIA
- Deloitte
- Proofpoint
- Rapid7
- Splunk
- Tenable
- VMware