SPONSORED CONTENT

Centralizing Cyber

States and localities increase coordination with the federal government

ADOBE STOCK

Mounting threats to critical infrastructure and vital services are remaking the cybersecurity relationship between states and localities and the federal government.

Two pieces of legislation approved over the past six months point toward a more centralized and coordinated approach to addressing cybersecurity vulnerabilities in the name of national security.

In November 2021, federal lawmakers approved dedicated funding for state and local government cybersecurity efforts, a move long sought by NASCIO and other groups. The new State and Local Cybersecurity Grant Program — included in the massive Infrastructure Investment and Jobs Act — provides $1 billion for cybersecurity improvements over four years.

Then, in March of this year, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 as part of the Consolidated Appropriations Act of 2022. The law will require providers of critical infrastructure services to report cyber incidents to the federal Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours.

Details for both measures are still being worked out. The Federal Emergency Management Agency is working with CISA to develop rules for awarding and distributing the new cybersecurity grants, which are expected to begin flowing to states late this year.

CISA is also responsible for figuring out how the new incident reporting law will work, including determining the thresholds for incident reporting and which organizations are subject to these requirements. This process will take longer. The law gives CISA two years to develop proposed rules and another 18 months to seek comment before finalizing them.

A More Active Federal Role

Taken together, these laws point toward significant changes in the nation's historically decentralized approach to cybersecurity.

"I think this is step one toward much more active federal involvement in state and local government cybersecurity programs," says *Government Technology* cybersecurity columnist Dan Lohrmann, former chief security officer and chief technology officer for the state of Michigan.

It's likely that state and local agencies will receive additional federal cybersecurity support going forward, along with greater federal oversight, Lohrmann says. "We're moving toward more involvement from national law enforcement and intelligence agencies, more funding and more mandates from the federal side."

He views the new cybersecurity grants as an important down payment on years of cybersecurity underinvestment and perhaps a template for ongoing federal funding for state and local cybersecurity protections. Although previous federal funding programs could be used to finance cybersecurity upgrades, those projects often lost out to competing priorities. The new grant program directs money specifically toward cybersecurity initiatives, enabling agencies to address what Lohrmann calls a "national debt in cyber" consisting of outdated systems, insecure software code and vulnerable networks.

"The grant program is significant. It's creating a new road for us," he says. "I think there will be more money in the future, and this is a model we'll be coming back to."

The incident reporting law will also trigger big changes. Although it doesn't take effect for a few years, Lohrmann expects the measure to drive new requirements for state and local agencies, particularly those providing services like electricity and drinking water.

"I believe mandatory reporting of cyber incidents will be coming to state and local governments, especially when they are performing functions that are deemed critical," he wrote in a *Government Technology* column published shortly before the legislation was signed into law. "My advice: Start getting ready for this now, if you haven't already built these scenarios into your

planning for business disruptions caused by a cyberattack.”

Facing New Threats

New cybersecurity legislation is being driven by a threat environment that seemingly grows more menacing by the day. The nation has weathered a wave of highly disruptive cyber events, including the Colonial Pipeline attack that threatened fuel deliveries to much of the southeastern U.S. in 2021.

Russia’s invasion of Ukraine adds new uncertainties. Security experts worry Russian cyber operations will attempt to disrupt critical state and local government services in retaliation for U.S. support of Ukraine. “There’s a belief that Russia may start causing us pain here," former CISA Director Christopher Krebs said during a recent *Government Technology* webcast.

Citing “evolving intelligence,” President Biden issued an urgent warning in March that the Russian government may launch malicious cyberattacks in response to crippling economic measures imposed on the country by the U.S. and its NATO allies. “It’s part of Russia’s playbook,” Biden said.

Picking Up the Pace

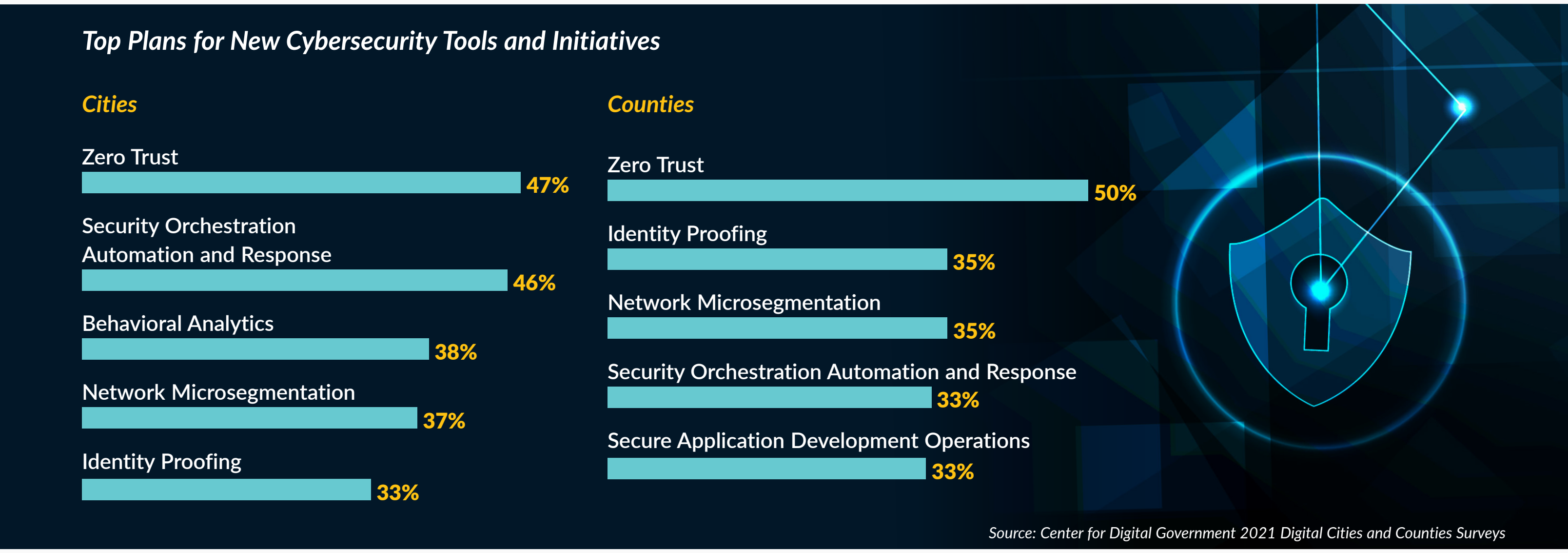
In response to these threats, government jurisdictions need to up their game on cyber. If they haven’t already, agencies should be assessing their current cyber risk and designing strategies to address vulnerabilities and strengthen security posture, Lohrmann says.

Some organizations have in-house resources to perform cybersecurity vulnerability assessments, but many others will need to consider working with partners. Organizations like CISA and the Center for Internet Security offer free resources. Commercial security vendors may also provide assessments for little or no cost, Lohrmann says.

In addition, agencies need a faster refresh cycle for cybersecurity strategies. Gone are the days when strategies remained effective for four to five years, he says. “My recommendation would be to comprehensively update your strategy every few years, at least, with smaller refreshes in between. Vulnerability assessments need to be refreshed regularly, too.”

Having a firm grasp on current cybersecurity needs and clear plans for addressing vulnerabilities will push agencies toward a stronger security posture. These moves also position agencies to compete effectively for upcoming cyber grants.

Successful grant applicants will show detailed plans for projects that move them toward Zero-Trust security environments, Lohrmann says. “The better you can quantify your gaps and lay out the case for filling them, the better your chances of getting the funds you need.”



Top Plans for New Cybersecurity Tools and Initiatives

Source: Center for Digital Government 2021 Digital Cities and Counties Surveys