Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Memorandum

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@state.co.us • leg.colorado.gov/lcs

February 22, 2022

TO: Joint Technology Committee Members

FROM: Colin Schroeder, Research and Committee Analyst, 303-866-3998
Joint Technology Committee Staff

SUBJECT: Summary of H.R. 3684, "Infrastructure Investment and Jobs Act," IT Components

Summary

The Infrastructure Investment and Jobs Act (IIJA) was signed into law by President Biden on November 15, 2021, and outlines various investments in the country's infrastructure programs. Contained within the law are several provisions specifically related to cybersecurity and information technology, which may be of interest to members of the Joint Technology Committee.

Contents

State and Local Cybersecurity Grant Program

The IIJA created a State and Local Cybersecurity Grant Program, administered by the U.S. Department of Homeland Security (DHS), which will award grants to states and tribal governments to help address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, and tribal governments.[1]

Funding and distribution. The U.S. Congress appropriated $1.0 billion over the next four federal fiscal years for this grant program. Of this amount, 1.0 percent is apportioned to each state, 0.25 percent is apportioned to each U.S. territory, and 3.0 percent is apportioned to tribal governments. The remaining amount is apportioned to states depending on each state's population and rural population.

State cybersecurity plans. States applying for a grant under this program must submit a cybersecurity plan to DHS that describes any existing state plans to protect against cybersecurity risks threats to information systems owned or operated by, or on behalf of, the state. The cybersecurity plan must

[1]H.R. 3684, Infrastructure Investment and Jobs Act, State and Local Cybersecurity Improvement Act, Section 70612

also involve consultation and feedback from local governments and associations of local governments within the state. These cybersecurity plans will be reviewed annually by DHS following an initial two-year approval.

The cybersecurity plan must describe, to the extent possible, how the state will:

- manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

- monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state;

- enhance the preparation, response, and resiliency of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats;

- implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state;

- ensure that the state and local governments within the state adopt and use best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology (NIST); cyber chain supply chain risk management best practices identified by the NIST; and knowledge bases of adversary tools and tactics;

- promote the delivery of safe, recognizable, and trustworthy online services by the state and local governments within the state, including through the use of the ".gov" internet domain;

- ensure continuity of operations of the state and local governments within the state in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident;

- use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity developed by the NIST to identify and mitigate any gaps in the cybersecurity workforces of the state and local governments, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state and local governments to address cybersecurity risks and threats, such as through cybersecurity hygiene training;

- ensure continuity of communications and data networks between the state and local governments in the event of an incident involving those communications or data networks;

- assess and mitigate, to the greatest degree possible, cybersecurity risks and threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the state;

- enhance capabilities to share cyber threat indicators and related information between the state and local governments, including by expanding information sharing agreements with DHS, and with DHS itself;

- leverage cybersecurity services offered by DHS;

- implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

- develop and coordinate strategies to address cybersecurity risks and threats in consultation with local governments and associations of local governments within the state, other neighboring states and tribal governments, and members of an information sharing and analysis organization;

- ensure adequate access to, and participation in, these services and programs by rural areas; and

- distribute funds, items, services, capabilities, or activities to local governments.

Finally, the cybersecurity plan must assess the capabilities of the state relating to the above actions; describe the individual responsibilities of the state and local governments in implementing the plan; outline the necessary resources and a timeline for implementing the plan; and describe the metrics the state will use to measure progress towards implementing the plan and reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the state or local governments.

In drafting its cybersecurity plan, a state may consult with the Multi-State Information Sharing and Analysis Center; include a description of cooperative programs developed by groups of local governments within the state to address cybersecurity risks and threats; and include a description of programs provided by the state to support local governments and owners and operators of critical infrastructure to address cybersecurity and threats.

Cybersecurity planning committee. States that receive a grant under this program must establish a cybersecurity planning committee to do the following:

- assist with the development, implementation, and revision of the state's cybersecurity plan;
- approve the state's cybersecurity plan; and
- assist with the determination of effective funding priorities for the grant.

Reporting. States that receive a grant under this program are required to submit an annual report to DHS that describes the progress of the state in implementing the state's cybersecurity plan and reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the state or local governments.

Cybersecurity for Critical Infrastructure

The IIJA provides guidance and support for several sectors of critical infrastructure with the purpose of protecting these sectors from cyberattacks and vulnerabilities.

Transportation. The law requires the Federal Highway Administration (FHA) to develop a tool to assist transportation authorities in identifying, detecting, protecting against, responding to, and recovering from cyber incidents. In developing this tool, the FHA is required to use the cybersecurity framework established by the NIST; establish a structured cybersecurity assessment and development program; coordinate with the Transportation Security Administration and the Cybersecurity and Infrastructure Security Agency; consult with the appropriate transportation authorities, operating agencies, industry stakeholders, and cybersecurity experts; and, provide for a period of public comment and review on the tool.

Additionally, the law expands the existing National Highway Performance Program and Surface Transportation Block Grant Program to allow program funds to be used to protect segments of the National Highway System and transportation facilities from cybersecurity threats.[2]

Energy. The law requires the Department of Energy (DOE) to create new programs to provide grants and technical assistance to improve utility providers' ability to detect, respond to, and recover from cybersecurity threats. The DOE must also create a program to develop advanced cybersecurity measures for the energy sector. Additionally, the DOE must create federal financial and technical assistance for states to implement an energy security plan, protecting states from cybersecurity threats to the energy infrastructure. Any recipient of funding may be required to establish a plan for maintaining and improving cybersecurity for the duration of the proposed project. Recipients of funding should maximize the use of open guidance and standards, including the Cybersecurity Capability Maturity Model, and the Framework for Improving Critical Infrastructure Cybersecurity of the NIST. Each submission for funding will be reviewed by the DOE Office of Cybersecurity, Energy Security, and Emergency Response.[3]

Broadband

The IIJA appropriates $42.45 billion for the "Broadband Equity, Access, and Deployment Program," to provide support and implementation of high speed wireless access for areas lacking broadband access. The bill also establishes a "middle mile" broadband infrastructure grant program, and

[2]H.R. 3684, Infrastructure Investment and Jobs Act, Sections 11510, 11105, and 11109.
[3]H.R. 3684, Infrastructure Investment and Jobs Act, Sections 40124, 40125, and 40126.

appropriates $1.0 billion to be used for grants for projects that will be capable of supporting retail broadband service, broadband mapping, or connection to anchor institutions.[4]

Digital Equity Act of 2021

The Digital Equity Act of 2021 included in the IIJA aims to close the digital divide amongst communities in the United States and reduce the disparities in digital proficiency. The law appropriates $2.75 billion in federal grant funds for digital equity over a five year period. As defined in the legislation, "digital equity" is "the condition in which individuals and communities have the information technology capacity that is needed for full participation in the society and economy of the United States."[5] To increase digital equity, the law establishes the following new grant programs to be administered by the National Telecommunications and Information Administration (NTIA).

State Digital Equity Capacity Grants. The law appropriates $1.5 billion for the State Digital Equity Capacity Grant Program to help states to implement State Digital Equity Plans. These plans must include: a report on barriers to digital equity faced by "covered populations" (covered populations include: low-income households, rural areas, senior citizens, veterans, racial/ethnic minorities, and individuals with disabilities or language barriers); measurable objectives for increasing access to wireless broadband technology; and a description of how the State plans to collaborate with stakeholders. The NTIA will award grants based on three criteria:

- 50 percent of the total grant amount will be based on the population of the eligible state, proportionate to the total population of all eligible states.
- 25 percent of the total grant amount will be based on the number of individuals in the eligible state who are members of covered populations proportionate to the total number of individuals in all eligible states who are members of covered populations.
- 25 percent of the total grant amount will be based on the comparative lack of availability of broadband in the eligible state, proportionate to the lack of availability of broadband in all eligible states.

These grants may be used to update or maintain the State Digital Equity Plan, implement the State Digital Equity Plan, and to pursue digital inclusion activities consistent with the State Digital Equity Plan.

Digital Equity Competitive Grants. The law appropriates $1.25 billion for the Digital Equity Competitive Grant Program to bolster efforts to achieve digital equity, promote digital inclusion activities, and foster more widespread adoption of broadband services for covered populations. Funds may be used to create training programs and workforce development programs, to provide free or low-cost equipment to covered populations, and to construct, upgrade, or expand public access computing centers.

[4]H.R. 3684, Infrastructure Investment and Jobs Act, Section 60102.
[5]H.R. 3684, Infrastructure Investment and Jobs Act, Digital Equity Act of 2021, Section 60301, *et seq.*

Cyber Incident Response

The law appropriates an additional $100.0 million to the Cyber Response and Recovery Fund.[6] These funds can be used for support of such activities as: vulnerability assessments and mitigation; technical incident mitigation; malware analysis; analytic support; threat detection and hunting; and network protections.

[6]H.R. 3684, Infrastructure Investment and Jobs Act, Section 70602.