IST POLICY MEMO | JUNE 2026

Last Mile Cybersecurity

By Nicholas Leiserson

Even though Congress recognizes that the United States' information technology (IT) and operational technology (OT) systems are highly vulnerable to cyber threats, the legislative branch has generally not included statutory cybersecurity requirements as part of significant funding bills.

The executive branch is little better at incorporating requirements. For more than a decade, successive administrations have made statements about the importance of cybersecurity in critical infrastructure, but the U.S. government has issued minimal guidance—and fewer requirements—for cybersecurity in federally-funded projects. To finally achieve last mile cybersecurity for IT and OT systems, Congress should consider several policy opportunities to better align stated cybersecurity goals with federal spending, including requiring changes to grant guidance, creating cybersecurity programs to support investments, or requiring set-asides within programs. Policymakers should also consider how to incorporate cybersecurity maintenance costs as part of projects.

The Cyber Threat Landscape

In April 2026, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory warning of ongoing cyber threats to U.S. critical infrastructure.[1] Amid U.S. combat operations in Iran, the advisory stated that pro-Iran regime hackers had infiltrated U.S. systems within the Government Services and Facilities (to include local municipalities), Water and Wastewater Systems (WWS), and Energy Sectors. At a time of war, America's adversaries were targeting the homeland through cyberspace.

This is not surprising. In 2023, government officials and cybersecurity firms revealed that People's Republic of China army units were infiltrating utilities and transportation hubs, pre-positioning in critical infrastructure in order to hold them at risk in the event of a conflict.[2] Whether to impede military mobilization or sow panic, connectivity puts domestic infrastructure on the front lines of conflict in cyberspace, a reality that is otherwise inconceivable in physical domains.[3]

At the same time, we face an array of other cyber threats. Cyber-enabled fraud cost Americans more than $20 billion in reported losses in 2025.[4] With respect to fraud associated with responses to the COVID-19 pandemic alone, estimates have put the cost at between $100-135 billion.[5] Cyber criminals are increasingly targeting organizations like schools and hospitals with extortion-based attacks. An average of five cyber incidents occur each week impacting K-12 schools,[6] and ransomware has shut down schools across the country.[7]

Collectively, these threats put our national and economic security at risk. When a hospital is shut down due to ransomware, patient outcomes suffer. Breaches of student data can affect children for their entire lives. What's more, recent advances in artificial intelligence tools have the potential to accelerate these significant challenges.

About the Institute for Security and Technology

The Institute for Security and Technology (IST) is the 501(c)(3) critical action think tank that unites technology and policy leaders to create solutions to emerging security challenges.

IST stands at the forefront of convening policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

About the Author

Nicholas Leiserson is the Senior Vice President for Policy at the Institute for Security and Technology (IST). A legislative strategist and technologist, he has spent 15 years addressing cybersecurity risk and resilience and managing multidisciplinary teams of senior professionals at the White House and on Capitol Hill.

Missed Opportunities: Federal Funding

The federal government plays a significant role in providing funding to help organizations, including hospitals, schools, water utilities, and state unemployment offices. This funding also extends to the purchase of information and communications technology and services (ICTS), which can be a target for malicious cyber actors. However, funding bills rarely address cybersecurity at all, much less require evaluation of those risks—and actions to address them—as a condition of receiving federal dollars. Consider several major spending bills from the last five years:

- **CARES Act (2020, $2.2T)**[8] - The Coronavirus Aid, Relief, and Economic Security (CARES) Act, the first major economic response to the COVID-19 pandemic, contains provisions to encourage remote doctor visits, as well as investments in telehealth and telework more broadly. Yet it only has three mentions of cybersecurity, two of which pertain to trainings for small businesses about risks associated with telework or remote customer service, and one of which is for CISA's pandemic efforts with critical infrastructure.
- **American Rescue Plan Act (2021, $1.9T)**[9] - The American Rescue Plan Act, passed in the early days of the Biden administration to respond to COVID-19, mentions cybersecurity in one provision, pertaining to funding for CISA to respond to the SolarWinds incident that had become public three months before passage.
- **Bipartisan Infrastructure Law (2021, $1.2T)**[10] - The Bipartisan Infrastructure Law (BIL) combined a traditional surface transportation reauthorization with more than $550 billion in additional infrastructure spending. It features several programs that are specifically targeted at making cybersecurity improvements, including $1 billion for state and local government cyber grants. However, with the exception of new programs at the Department of Energy (discussed below), only one of the non-cybersecurity-focused programs requires cybersecurity to be considered at all.[11] At most, some programs explicitly list cybersecurity technologies as an allowable use of funds, but program administrators are neither required nor even encouraged to make cybersecurity assessments of the projects they approve.
- **Inflation Reduction Act (2022, $891B)**[12] - The Inflation Reduction Act, which made substantial investments in energy infrastructure and climate change mitigation, has no mentions of cybersecurity whatsoever. This is despite the inclusion of provisions covering topics from apprenticeships to critical minerals sourcing requirements.
- **One Big Beautiful Bill Act (2025, $3.7T)**[13] - While primarily a tax bill, the One Big Beautiful Bill Act contains hundreds of billions in new funding for national security priorities. Despite the focus on building the defense industrial base, other than a $90 million appropriation for assistance to small, non-traditional contractors that mentions cybersecurity, there are no other mentions beyond USCYBERCOM and existing programs of record.

Taken collectively, these laws expose a significant gap. Despite the risks evident to U.S. critical infrastructure in the cyber domain, Congress rarely includes explicit requirements to address cybersecurity as part of funding legislation.

Missed Opportunities: Executive Branch Efforts

Executive branch agencies regularly add conditions to funding beyond those imposed in statute by Congress. However, both regulatory and non-regulatory approaches fail to address core elements of cyber risk as a condition of receiving funding.

REGULATORY EFFORTS

Depending on the type of project, there are two primary regulations that govern requirements for receiving federal funding.

The primary regulation governing requirements for grants, including pass-through grants to states, which encompasses much of traditional infrastructure spending, is the Uniform Guidance for Federal Awards ("Uniform Guidance"), issued by the Office of Management and Budget (OMB).[14] In its 2024 update,[15] OMB explicitly calls out cybersecurity as a risk factor for grant-making agencies to consider before making an award. The 2024 update required recipients and sub-recipients to take documented steps to mitigate cybersecurity risks to sensitive information. And, for the first time, OMB explicitly added cybersecurity as a potential direct cost for grantees. In other words, grantees can now incorporate the costs of cybersecurity controls into their grant budgets, as opposed to taking money for cybersecurity out of the limited amount of administrative overhead allowed for a particular grant award.

However, these changes—and the guidance itself—are focused on protecting federal information, not the projects themselves. As a result, the most stringent requirements for states focus on efforts to protect sensitive data about law enforcement investigations[16] and tax records,[17] *not on the critical functions that state and local governments perform*.[18]

The story is similar on the contracting front, where requirements derive from the Federal Acquisition Regulation (FAR). In 2021, President Biden's Executive Order 14028[19] called for revisions to the FAR that would raise the cybersecurity bar for contractors, mandating uniform baseline cybersecurity requirements across agencies. Five years later, those reforms remain pending.

Even where there has been regulatory progress, such as with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) Program,[20] the focus remains on protecting the confidentiality of government data stored on contractor systems. Cybersecurity requirements for the systems themselves are handled on a case-by-case basis—and are generally not addressed at all.

NON-REGULATORY EFFORTS

There are other, less formal measures that agencies can take to encourage the evaluation of cybersecurity as part of funding decisions. However, there is limited evidence that these measures are driving behavioral change.

For example, notices of funding opportunity (NOFOs) tied to programs in the 2021 Bipartisan Infrastructure Law were one route the Biden administration tried to use to encourage the evaluation of cybersecurity as part of funding decisions. Following passage of the BIL, the administration decided that NOFOs tied to programs supported in the bill would need to contain language explicitly calling out cybersecurity.[21] However, as a practical matter, NOFO clauses requiring that there be "an effort to consider and address" cyber risks are very difficult to enforce. There is no definition of what is sufficient to meet the threshold for considering and addressing cyber risks, which makes it challenging for both potential grantees and federal program officers to assess whether a project proposal satisfies this directive. What's more, there is no corresponding language that exists in the grant terms and conditions, making it challenging to ensure that any planned cybersecurity mitigations are actually put in place.

In December 2024, the Office of the National Cyber Director (ONCD) and CISA put out a "Playbook for Strengthening Cybersecurity for Federal Grant Programs in Critical Infrastructure" ("ONCD Playbook"),[22] which was intended to address some of the shortcomings of the NOFO-only approach. The playbook has guidance for federal program officers, grant recipients, and even state pass-through entities on how to incorporate cybersecurity into their project lifecycles, including sample risk management plans and boilerplate terms and conditions. However, the playbook has not been widely adopted, and attempts to incorporate it into the Uniform Guidance as a requirement for awards above a certain dollar amount were rebuffed at the end of the Biden administration.

Policy Approaches

Policymakers looking to address gaps in critical infrastructure cybersecurity should consider leveraging the federal government's spending power, whether through grant-making or acquisition requirements. In doing so, they should be cognizant of the limitations that constrain existing efforts, and they should also ensure that approaches reflect the recurring nature of cybersecurity expenses.

Agency-Specific Plans: The Section 40126 Approach

One bright spot in the funding bills considered above is Section 40126 of the BIL, which sets out a framework for the Secretary of Energy to require cybersecurity plans for *all* of the Department's programs included in the BIL. Importantly, the law requires the Department to consider both the cybersecurity maturity of the grant recipient and the solutions funded by the Department of Energy.

There are several advantages with this approach. Setting a blanket requirement at the agency level consolidates cybersecurity expertise (in the case of 40126, the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, is tasked with reviewing the cybersecurity plans) and also allows for sector-specific requirements (e.g., protection of information related to the bulk power system) that may not fit within a government-wide mandate. The review by CESER also ensures that independent cybersecurity experts are evaluating plans for adequacy, rather than program officers who might have other objectives they are trying to achieve.

However, there are real challenges with the 40126 approach. First and foremost, the framework itself is not mandatory. While the Department of Energy continues to require 40126 cybersecurity plans today,[23] this requirement is reliant on the Secretary's discretion. Framing it as "the Secretary may require" [emphasis added] is inadequate in light of the current risk environment. The plans are also not self-executing. CESER's templates[24] help identify different areas of risk that a project should account for, but they stop at "high-level descriptions" and do not require any details that would facilitate holding grantees accountable for their plans. Lastly, while the templates do mention resourcing, they fail to include specifics, which may result in inadequate funding being set aside for cybersecurity purposes.

Addressing issues on an agency-by-agency basis may prove more tractable than other approaches, as it requires less inter-committee or interagency coordination. Section 40126 provides a starting point for policymakers, but it also offers lessons learned: policymakers should consider making plans mandatory and incorporating the ability to audit and hold grantees accountable after funding is awarded.

A Broad Baseline: Applying the Playbook

Another approach for policymakers could be to use the ONCD Playbook as a starting point for setting universal cybersecurity risk mitigation requirements as part of federal awards. Updates to the Uniform Guidance[25] could then require that all agencies include cybersecurity terms and conditions that, at minimum, cover the elements of the ONCD Playbook. In instances like transportation or

healthcare funding, which require non-federal entities to go through their own contractual processes, these terms and conditions would also be passed down to those sub-awardees. Changes to the Uniform Guidance could be effectuated within OMB, through the Office of Federal Financial Management, or through statutory requirements advanced by Congress.

A uniform requirement has several advantages. Lack of regulatory harmonization continues to plague policymakers,[26] and differing agency requirements relating to the protection of federal information impose a major cost on states. A government-wide approach avoids the proliferation of confusing or conflicting guidance and simplifies training for federal program officers and potential awardees. Uniformity also helps build a shared culture recognizing the importance of cybersecurity, rather than relegating it to only being the concern of specific agencies, such as those with national security mandates.

There are drawbacks with this approach. Centralization can increase efficiency, but it also may mean teams offering technical assistance lack domain knowledge (e.g., with respect to power systems). Given recent cuts to CISA,[27] there might not be capacity to offer assistance to other agencies for some time. Given the large number of agency equities potentially impacted, advancing a whole-of-government approach may also prove challenging without a strong push from the White House or Congressional leadership.

Create a Cyber Set-Aside

Rather than addressing programs directly in statute or regulations, policymakers might consider allocating a set proportion of federal program funds used for ICTS to meet cybersecurity needs. While estimates vary, surveys of chief information security officers in industry reflect that approximately 10 percent of IT spending is used for security.[28] Congress could consider a similar target and leave it up to agencies to design both policies to implement a set-aside and evaluation metrics to ensure they reach the target.

By ensuring that the funding for cybersecurity is available without prescribing how it should be used, this approach provides maximal flexibility to evolve over time. A flat set-aside addresses a core concern with other approaches: namely, the interests of program officers and grantees are not always aligned with those of policymakers seeking to improve cybersecurity. Without a set-aside, spending less on cybersecurity now frees up funding for other projects, potentially incentivizing under-investment in cybersecurity. The risk of that underinvestment falls not on the program officers and grantees making those spending decisions, but on the public, whose critical infrastructure could be made vulnerable for years (or decades) to come. A set-aside removes this misalignment by ensuring that cybersecurity receives adequate funding, regardless of any perverse incentives to under-spend relative to risk.

The challenge with this approach is that it is not risk-based. Using a heuristic means that some proportion of projects will end up with more cybersecurity funding than they actually need to match their risk profile.[29] Policymakers will have to weigh that inefficiency against the significant effort it takes to produce cybersecurity risk management plans that are attempting to capture something that is inherently difficult to measure. Under a set-aside regime, more dollars could be devoted to implementing cybersecurity improvements rather than attempting to justify them. Policymakers should also consider whether the flexibility afforded by over-investing in some cases is actually a net benefit, as rapid changes in the threat landscape[30] can quickly invalidate earlier risk assessments.

A Note On Implementation

To aid policymakers looking to implement any of the approaches in this memo, potential legislative or regulatory language can be found **on the IST website**. The below example demonstrates one way to implement the Cyber Set-Aside approach in a program authorization.

"Sec. Cybersecurity Funding Required—Of the funding used by awardees for information and communications technology and services, not less than 10 percent shall be used for a cybersecurity purpose, as that term is defined in Section 2200 of the Homeland Security Act of 2002 (6 USC 650)."

Additional Considerations

Combining Approaches

The approaches outlined above are not mutually exclusive. For instance, Congress could create a funding set-aside that the administration implements in part using the ONCD Playbook. Agency heads could act on their own volition to use the ONCD Playbook for any awards they make. Policymakers will have to choose among the tradeoffs of the different approaches, but they can be combined and begun in parallel.

Maintenance Considerations

A core challenge that policymakers will need to address is that cybersecurity investments are simultaneously essential during the build out of critical infrastructure projects and also insufficient. Investments in security-by-design,[31] the migration of legacy systems to the cloud, and network

security appliances can all significantly improve the cybersecurity posture of a project. However, many core cybersecurity capabilities, such as identity and access management (IAM) or endpoint detection and response (EDR), are not a one-time, upfront cost, but a continuous investment provided through termed licenses. Any effort to improve the security of federally-funded projects must also consider lifetime costs for services—as well as the cost of the people necessary to monitor these sensors and take steps to remediate deficiencies. Policymakers may wish to consider requiring that end operators of projects also demonstrate their plans for cybersecurity operationally and financially over the lifetime of the project. For example, in the case of a light rail system, the city, as the end user, should be responsible for demonstrating its plan to make expenditures supporting the system's cybersecurity posture across its lifetime.

Way Forward

Major funding legislation, including the surface transportation authorization and the Farm bill, is expected to be considered in this session of Congress. Congressional leadership may also take up another reconciliation bill that could spend hundreds of billions on new defense systems. These efforts will make meaningful investments in critical infrastructure that is connected—and therefore vulnerable. What's more, advances in AI, changes in the geopolitical landscape, or acute crises may give rise to new funding proposals. Policymakers should take the opportunity now to consider how to ensure that cybersecurity goals set in national strategy are carried out all the way to the "last mile," where federal dollars are translated into critical infrastructure.

The Institute for Security and Technology is grateful for the support of CrowdStrike, whose funding supported efforts to pursue this research.

Endnotes

1 https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a
2 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
3 https://chinaselectcommittee.house.gov/about/events/hearing-ccp-cyber-threat-american-homeland-and-national-security
4 https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions
5 https://www.gao.gov/products/gao-23-106696
6 https://www.k12six.org/map
7 https://www.k12dive.com/news/school-ransomware-attacks-cybersecurity-funding/730333/
8 https://www.govinfo.gov/content/pkg/PLAW-116publ136/pdf/PLAW-116publ136.pdf
9 https://www.govinfo.gov/content/pkg/COMPS-16472/pdf/COMPS-16472.pdf
10 https://www.govinfo.gov/content/pkg/PLAW-117publ58/pdf/PLAW-117publ58.pdf
11 It is explicitly called out as part of the vehicle-charging infrastructure grants, where potential grantees will need to show they've worked with stakeholders to address cybersecurity considerations in order to be eligible for an award.
12 https://www.govinfo.gov/content/pkg/PLAW-117publ169/pdf/PLAW-117publ169.pdf
13 https://www.govinfo.gov/content/pkg/PLAW-119publ21/pdf/PLAW-119publ21.pdf
14 https://www.congress.gov/crs-product/IF13138
15 https://www.federalregister.gov/documents/2024/04/22/2024-07496/guidance-for-federal-financial-assistance?
16 https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center
17 https://www.irs.gov/pub/irs-pdf/p1075.pdf
18 https://www.cisa.gov/topics/risk-management/national-critical-functions
19 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
20 https://dodcio.defense.gov/CMMC/
21 The language generally matched this form: "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against all hazards, including physical and cyber risks, consistent with Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience, and the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Each applicant selected for NSFLTP [the program] funding must demonstrate, prior to the signing of the grant agreement, an effort to consider and address physical and cyber security risks relevant to the

transportation mode, type, and scale of the project. Projects that have not appropriately considered and addressed physical and cyber security and resilience in their planning, design, and project oversight, as determined by DOT [the agency] and the U.S. Department of Homeland Security, will be required to do so before receiving funds." https://highways.dot.gov/media/55386

22 https://www.cisa.gov/sites/default/files/2024-12/Playbook%20for%20Strengthening%20Cybersecurity%20in%20Federal%20Grant%20Programs%20508.pdf

23 https://infrastructure-exchange.energy.gov/FileContent.aspx?FileID=f5841d12-7e64-4788-a938-f7867eda809b

24 https://www.energy.gov/ceser/infrastructure-investment-and-jobs-act-implementation

25 Policymakers may also consider similar updates to the FAR for projects where ownership will finally transfer to the U.S. government.

26 https://www.hsgac.senate.gov/hearings/streamlining-the-federal-cybersecurity-regulatory-process-the-path-to-harmonization/

27 https://www.cybersecuritydive.com/news/cisa-departures-trump-workforce-purge/749796/

28 https://www.iansresearch.com/resources/press-releases/detail/new-research-from-ians-and-artico-search-reveals-cybersecurity-budgets-increased-just-6-for-2022-2023-cycle.

29 Projects with a risk profile that requires more investment than the baseline may end up being shortchanged, with less funding allocated than is appropriate. However, a set-aside is a floor, not a ceiling, for funding. A risk-based approach, as contemplated in the other courses of action, could sit atop the set-aside for particularly high-risk projects to ensure they receive the supplementary investments they need.

30 https://www.anthropic.com/glasswing

31 https://www.cisa.gov/securebydesign