Chairman Peters
Ranking Member Portman
Committee on Homeland Security and Governmental Affairs
U.S. Senate

Chairwoman Cantwell
Ranking Member Wicker
Committee on Commerce, Science, and Transportation
U.S. Senate

Chairman Thompson
Ranking Member Katko
Committee on Homeland Security
U.S. House of Representatives

Chairman DeFazio
Ranking Member Graves:
Committee on Transportation and Infrastructure
U.S. House of Representatives

The Honorable Shalanda Young
Director of the Office of Management and Budget

May 20, 2021

We the undersigned respectfully urge Congress and the Administration to ensure cybersecurity is integrated into planned infrastructure modernization efforts such as the American Jobs Plan. We recommend incorporating cybersecurity-specific funding, incentives, and risk-based minimum standards into infrastructure legislation and its implementation to ensure we are not building next-generation infrastructure with last-generation security.

The White House recently announced cybersecurity funding and standards will be incorporated into the American Jobs Plan.[1] We support the items outlined by the White House, urge their inclusion in the final legislation, and encourage the Administration and Congress to take additional steps to secure all types of critical infrastructure in the American Jobs Plan.

[1] White House, Fact Sheet: The American Jobs Plan Will Bolster Cybersecurity, May 18, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/18/fact-sheet-the-american-jobs-plan-will-bolster-cybersecurity.

Updating the United States' critical infrastructure is essential to long term economic prosperity, global competitiveness, and job growth. However, these benefits will be significantly undermined, and the US will face prolonged risks to health, safety, and national security, if cybersecurity is not a high priority for new infrastructure projects at the start. The past six months alone provide several reminders of the sobering risks US critical infrastructure faces: ransomware leading to the temporary shutdown of a crucial US fuel pipeline, ongoing attacks against healthcare providers, the incident at the Florida water treatment facility, election security threats, multiple supply chain attacks, and severe compromises to government systems.

Upgrading our smart infrastructure will substantially increase our technology footprint. Without strong security, this will make existing unaddressed weaknesses even more dangerous by creating a larger attack surface for malicious actors and adversary nations. It will be more difficult to bolt security onto critical infrastructure after the fact than to modernize infrastructure with security in mind from the beginning. Enhancing breach notification or cyber incident reporting requirements for affected companies may aid threat intelligence, but will not prevent those incidents from occurring as effectively as integrating security safeguards and processes early on.

The need for funding, incentives, and minimum standards applies to federal, state, local, and privately held infrastructure. Upgrading the security of government agencies and contractors is crucial, but strengthened cybersecurity should also be prioritized for privately held critical infrastructure (which is the overwhelming majority of US critical infrastructure). Yet many critical infrastructure entities are under-resourced and, in some cases, have security maturity that is not commensurate with the risks and threats they face.

We strongly recommend that the infrastructure modernization legislation, and implementation of this legislation, include cybersecurity-specific funding for federal, state, local, and privately held infrastructure. This may include grants and other resources specifically dedicated to strengthening critical infrastructure entities' security processes, workforce, and technology, so that the funds are not allocated for other priorities. We also recommend tying baseline cybersecurity processes and safeguards, such as the NIST Framework to Improve Critical Infrastructure Cybersecurity, to new mandated critical infrastructure projects and modernization funds. To ensure security is accounted for while providing adequate flexibility for businesses, cybersecurity requirements for critical infrastructure should be based on risks, tailored to the specific sector, aligned with existing standards, and be neither unduly burdensome nor unnecessary.

We commend the Administration for making clear to Congress that cybersecurity must be a priority in the American Jobs Plan.[2] We support inclusion of the items announced by the White House in the legislation, though note that these items relate largely to the energy sector. Bolstered energy sector and electric grid resilience is crucial to US security and competitiveness, but cybersecurity should also be prioritized for the other critical infrastructure sectors - such as water, critical manufacturing, and healthcare.[3]

We suggest the Administration consider taking additional steps to detail how the Administration intends to integrate cybersecurity into the implementation of the American Jobs Plan:

1. The Office of Management and Budget (OMB) should commit to directing a portion of resources allocated for federal Sector Risk Management Agencies under the American Jobs Plan to funding safeguards and processes to improve the security posture of all US critical infrastructure sectors.[4]

2. OMB should commit to tying eligibility for federal grant funds for critical infrastructure to adoption of risk management standards and best practices, such as the NIST Cybersecurity Framework, as is already required of federal government agencies pursuant to Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[5]

In addition to the Administration's actions, we suggest that Congress integrate the following into infrastructure modernization legislation:

1. The *State and Local Cybersecurity Improvement Act*, which would establish grants to states to address cybersecurity risks to both state and critical infrastructure information systems, and require grant recipients to implement risk management processes

---

[2] White House, Fact Sheet: The American Jobs Plan Will Bolster Cybersecurity, May 18, 2021.
[3] Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Sectors, https://www.cisa.gov/critical-infrastructure-sectors.
[4] For example, Transportation Secretary Buttigieg indicated that cybersecurity may be considered as a requirement for grants under the American Jobs Plan. White House Press Briefing, May 12, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/12/press-briefing-by-press-secretary-jen-psaki-secretary-of-transportation-pete-buttigieg-and-administrator-of-the-u-s-environmental-protection-agency-michael-regan-may-12-2021.
[5] For example, the Department of Homeland Security recently announced expansion of its preparedness grants to include cybersecurity, several of which require or encourage adoption of the NIST Cybersecurity Framework. See DHS Announces Funding Opportunity for $1.87 Billion in Preparedness Grants, Feb. 25, 2021, https://www.dhs.gov/news/2021/02/25/dhs-announces-funding-opportunity-187-billion-preparedness-grants. See also, FEMA Preparedness Grants Manual v2, Feb. 2021, Intercity Passenger Rail Program, Intercity Bus Security Grant Program.

consistent with the NIST Cybersecurity Framework.[6]

2. The *Protecting Resources On The Electric grid with Cybersecurity Technology Act*, which would provide incentives to electric utilities to invest in cybersecurity, and establish grant and assistance programs for utilities to deploy stronger cybersecurity safeguards.[7]

3. Increase the 302(b) allocation, specifically the 050 budget funding allocation, for the Cybersecurity and Infrastructure Security Agency (CISA), as recommended by members of the US Cyberspace Solarium,[8] to expand CISA's capacity to engage all critical infrastructure sectors, among other things.

4. Incentivize close alignment with the NIST Cybersecurity Framework and other key security standards by mitigating fines for compliant critical infrastructure entities.[9]

5. Fund and provide authority for CISA to develop and administer information security education and training programs. This should include entry and mid-level education, as well as industrial control system (ICS) training programs for all utilities, including water and wastewater throughout the US.[10]

6. The *Advancing CDM Act*, which would support and secure the federal digital infrastructure by expanding the federal Continuous Diagnostics and Mitigation (CDM) program to cover federal agency operational technology and industrial control systems (OT/ICS), and requiring the implementation of risk-based vulnerability management practices.[11]

7. Expand the Department of Defense (DoD) Assured Compliance Assessment Solution (ACAS) program to include OT/ICS sensors and direct the DoD to include OT/ICS in cybersecurity assessment and inspection criteria.[12]

---

[6] H.R. 3138 - 117th Cong.
[7] S.1400 - 117th Cong.
[8] Letter from Reps. Mike Gallagher and James Langevin to House Committee on Appropriations Chairwoman DeLauro and Ranking Member Granger, Apr. 22, 2021, https://langevin.house.gov/sites/langevin.house.gov/files/documents/21-04-23%20Cyberspace%20Solarium%20302%28b%29%20Homeland%20Allocation%20Letter.pdf.
[9] Ransomware Task Force, Combating Ransomware, Apr. 29, 2021, recommendation 3.4.4, https://securityandtechnology.org/ransomwaretaskforce/report.
[10] Testimony of Chris Krebs before the US House Committee on Homeland Security, Feb. 10, 2021, pg. 6, https://homeland.house.gov/download/krebs-testimony-cyber-21021.
[11] S.2318 - 116th Cong.
[12] Defense Information Systems Agency, Assured Compliance Assessment Solution, https://storefront.disa.mil/kinetic/disa/service-catalog#/category/cyber-security#section_assessments-and-inspections.

8. Incorporate OT/ICS system security into the CISA National Cybersecurity Assessments and Technical Services (NCATS) program for critical infrastructure[13].

We the undersigned respectfully encourage Congress and the Administration to work together urgently to ensure US critical infrastructure sectors have the resources, incentives, and standards necessary to modernize securely. Strengthened cybersecurity will be an investment in US businesses that rely on critical infrastructure, and help government entities to be more modern and efficient. Thank you for your consideration.

Rapid7
Alliance for Digital Innovation
Avast
Broadcom
Bugcrowd
Citrix
Cybereason
Cybersecurity Coalition
Cyber Threat Alliance
Disclose.io
Global Cyber Alliance
GRIMM
ICS Village
Institute for Security and Technology
Luta Security
McAfee
SCYTHE
SecurityScorecard
Tenable

[13] CISA, National Cybersecurity Assessments and Technical Services, https://us-cert.cisa.gov/resources/ncats.

Cc:
The Honorable Alejandro Mayorkas
The Honorable Ron Klain
The Honorable Susan Rice
The Honorable Jake Sullivan
Majority Leader Schumer
Minority Leader McConnell
Speaker Pelosi
Minority Leader McCarthy