Tab 1

Executive Chamber

KATHY HOCHUL
Governor

COLIN AHERN
Director of Security and Intelligence

State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities

U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Testimony of:
Mr. Colin Ahern
Director of Security and Intelligence
New York State

Washington, DC
May 21, 2026

INTRODUCTION

Chairman Ogles, Ranking Member Ramirez, Chairman Garbarino, Ranking Member Thompson, and distinguished Members of the Subcommittee:

Thank you for the opportunity to submit testimony on the state of cybersecurity at the state and local level, the escalating threats facing America's communities, and the federal partnership needed to defend them.

Given the escalating threats we face today, this hearing could not be more urgent. Our states are on the front lines of multiple cyber conflicts, yet we are being asked to manage nation-state risks while our federal partners step back. It is a strategic failure that our primary federal partners and resources are being sidelined as threats escalate. From the imminent expiration of the State and Local Cybersecurity Grant Program (SLCGP), the shrinking of the Cybersecurity and Infrastructure Security Agency (CISA) and the lack of a Senate-confirmed CISA Director, to the cancellation of funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC), tools designed to keep our communities safe are being dismantled.

A functional partnership between federal, state and local governments, and the private sector is essential to reverse this trend. This partnership must be built on three key pillars. First, we need a Federal Government capable of detecting, mitigating, and responding to cyberattacks and deterring and punishing attackers across the operational spectrum. Second, we require robust collaboration with state and local governments and the private sector that facilitate rapid information exchange and operational coordination. Third, we need a private sector capable of defending its own systems and preventing attacks from originating within its infrastructure.

Currently, these pillars are being systematically undermined. Over the past year, the Trump administration has reduced funding for key offices and decommissioned collaboration mechanisms critical to our collective defense. By failing to address the risks of frontier AI, the administration has allowed the gap between the capability of nation-states and the capability of terrorist and criminal actors to vanish. This leaves under-resourced state and local governments, school districts, water utilities, and others

to face sophisticated adversaries alone. Without federal coordination for vulnerability disclosures, replacing legacy systems, and improved cyber defensive methodologies, we risk substantial, irreparable harm to our economy and our democratic way of life.

The State and Local Cybersecurity Grant Program has been a critical resource for state and local governments to defend our communities and continue to provide the services that the private sector and our people rely on. This program should be reauthorized and funded for the long term to provide sustained, stable resources to state and local governments facing growing threats.

My testimony outlines the threat landscape from the perspective of one of the largest states in the country and offers insights on our unique whole-of-state response and the results it has produced. I also lay out six recommendations for this Subcommittee and your colleagues in Congress to improve the resilience of America's communities by building better federal and state government partnerships.

I. THE THREAT LANDSCAPE

The cyber threat environment in 2026 is primarily being reshaped by two parallel forces. The first is a sustained, multi-vector campaign against U.S. critical infrastructure by nation-state, nation-state affiliated and supported adversaries, and transnational cybercriminals. The second is a rapid expansion of offensive capability driven by the maturation of frontier artificial intelligence (AI) and powerful open-weight models, in addition to the continued proliferation of highly professionalized cyber offensive capabilities to criminals and terrorists. Each of these forces is dangerous on its own. Together, they constitute the most consequential shift in the cyber threat picture since the emergence of nation-state cyber operations thirty years ago and the explosion of professional cybercriminal organizations with the advent of cryptocurrency fifteen years ago.

States are at the front lines of cyberattacks. New York’s history as a target of America’s adversaries is long and varied, stretching from the physical attacks on the World Trade Center; the cyber campaigns against our financial industry; and the scams targeting our

residents. Today, these physical and cyber threats have metastasized into a converged cyber-physical assault on our essential infrastructure. The public authorities, state and local governments, and municipal utilities that provide essential services like transportation, power, and clean water are being targeted by adversaries who do not respect state lines or national borders. We would never expect a local portmaster to repel a foreign warship steaming into a harbor, yet we leave the operational fabric of our communities to fend for themselves against the world's most sophisticated digital adversaries.

A. The Artificial Intelligence Inflection

Technical barriers that once limited sophisticated offensive cyber capabilities to an elite few are breaking down. Frontier AI and open-weight models, in their current generation, are already providing operational gains for our adversaries: the time from vulnerability discovery to working exploits has collapsed from weeks to hours;[1] thanks to deepfakes and other AI-enabled techniques, phishing emails can be nearly impossible to detect and are turbocharging ransomware attacks;[2] and sophisticated cyberattacks overall are rapidly increasing in frequency.[3] Without meaningful safety constraints on these models, including those controlled by competitors such as China,[4] the time, effort, and skill required for sophisticated cyber operations will exponentially decrease over the next six months, effectively democratizing sophisticated offensive cyber capabilities. The capability distinction between highly resourced and capable nation-state adversaries and everyone else – individuals, small groups, terrorist organizations, professionalized cybercriminals, and other non-nation state actors – is bound to collapse; the threat posed by actors capable of increasingly damaging and frequent cyberattacks will grow exponentially.

Traditional deterrence, which is already severely lacking, will fail completely in this modern threat environment. Non-state threat actors may be equipped with nation-state level capabilities with AI, but they are not bound by the same geopolitical or legal

[1] https://www.ibm.com/think/insights/the-mythos-moment-when-discovery-outpaces-defense
[2] https://go.crowdstrike.com/2026-global-threat-report.html
[3] https://mitsloan.mit.edu/ideas-made-to-matter/ai-cyberattacks-three-pillars-defense
[4] https://www.nist.gov/news-events/news/2026/05/caisi-evaluation-deepseek-v4-pro

pressures that deter nation-state adversaries from carrying out truly devastating cyberattacks on critical infrastructure. Because these non-state actors often operate outside this reach of conventional statecraft, we must focus even more forcefully on hardening our defenses to ensure attacks cannot succeed, and that we can rapidly recover from those that do.

To meet this challenge, we must mature our technology systems. At the state and local level, entities are plagued by legacy infrastructure and outdated technologies. Under-resourced critical infrastructure providers, school districts, and electrical and water utilities are already under severe strain from traditional adversaries, especially ransomware and were never designed to withstand a landscape of highly capable, AI-powered threat actors. This is why sustained federal resources through the PILLAR Act and the State and Local Cybersecurity Grant Program are essential, providing the funding needed to modernize fragile systems and deploy enterprise-grade defenses across our state and local governments. The time to act is now.

B. Nation-State Threats

Nation state threats have continued to advance against the United States and New York specifically. While their operational priorities differ, the strategic pattern is consistent: Nation state cyber threats are no longer limited to traditional espionage. They have expanded into three categories: prepositioning for destructive cyberattacks in critical infrastructure;[5] the theft of intellectual property and economic assets;[6] and the use of cyber capabilities to extend transnational coercion into our communities and generate revenue.[7]

Four nation-state actors drive the bulk of this activity: the People's Republic of China (PRC), the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea (DPRK). PRC operations have been publicly identified across U.S. telecommunications, water and wastewater, and energy sector systems, with March 2025 federal indictments confirming that Beijing operates a contractor

[5] https://www.congress.gov/crs-product/IF12798
[6] https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says
[7] https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforce ment-officers-global

ecosystem that serves as both an intelligence platform and a transnational repression apparatus. Russia continues to function as the principal sanctuary jurisdiction for the criminal ransomware ecosystem.[8] Iranian cyber activity continues to target energy, transportation, water, and government services.[9] DPRK cyber operations combine cryptocurrency theft and fraud, such as remote worker scams.[10]

Across all three categories, the convergence between criminal and state-aligned cyber activity described elsewhere in this testimony is no longer occasional. It is systemic. The same infrastructure, the same intermediaries, and increasingly the same techniques serve nation-state actors and the criminal ecosystems that operate adjacent to them. The defensive posture required to address active prepositioning, sustained theft, and adaptive coercion campaigns must operate continuously, with sustained federal partnership, sustained intelligence sharing, and sustained investment in the state and local capacity that defends the infrastructure and communities the Federal Government cannot reach directly.

C. Criminal Threats

The criminal threat surface is broad, lucrative, and accelerating. Phishing is the top cyber incident category reported to the State, and the days of ill-crafted phishing emails are long over. Cybercriminal groups now produce highly credible, often personalized lures that enable downstream fraud, data theft, and ransomware deployment.

The financial harm to New Yorkers is substantial. In 2025, the FBI's Internet Crime Complaint Center (IC3) ranked New York as the fourth among states in the following metrics: total reported complaint volume (45,255 complaints) and total victim losses (over $1.2 billion); cryptocurrency-related complaints (8,088 complaints) and related losses (nearly $600 million); and elder fraud losses (over $408 million).[11] The single

[8] https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-net work-controlled
[9] https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations
[10] https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-techology-worker-0
[11] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

largest driver of those losses is investment fraud, dominated by the relationship-based cryptocurrency scams commonly called "pig butchering." The FBI attributes these schemes specifically to organized criminal enterprises operating from Southeast Asia, using trafficked workers as forced labor.

The theme again is one of convergence. The same criminal infrastructure that enables pig butchering also enables state-sponsored IT worker schemes, ransomware operations, and nation-state actors who obtain capabilities from professional criminal markets. Cryptocurrency mixers launder ransomware and investment-fraud proceeds. Cloud hosting providers enable both criminal and nation-state operators. Identity-laundering services supply both cybercriminal fraud rings and nation-state cyber operations. New York's 2023 Cybersecurity Strategy described this as the “convergence of criminal and nation-state actors.”[12] Three years on, that convergence is sharper, faster, and more difficult to disrupt. Treating cybercriminals and nation-state cyber threats as separate problems is a mistake, as they sit on top of the same plumbing, and federal action against both requires dismantling the infrastructure that serves them all.

II. NEW YORK’S WHOLE-OF-STATE RESPONSE

Governor Hochul's establishment of the Director of Security and Intelligence role in February 2026[13] built on several years of sustained investment in the State's cyber and hybrid threat capabilities, organized around the framework set out in the 2023 New York Cybersecurity Strategy and its principles of unification, resilience, and preparedness. The State's current operational posture rests on five mutually reinforcing components, each outlined in this section. Taken together, they constitute a model that other states are beginning to follow and that this Subcommittee should consider as a template for federal-state cyber partnership.

A. Unified Governance

The State has consolidated cyber, intelligence, and foreign-influence functions under unified senior leadership. This centralized structure allows the State to act coherently

[12] https://www.governor.ny.gov/sites/default/files/2023-08/2023-NewYork-CybersecurityStrategy.pdf
[13] https://www.governor.ny.gov/news/governor-hochul-appoints-new-york-states-first-ever-director-security-and-intelligence

when threats cross domains. It has also enabled the development of policies and programs which provide cybersecurity shared services to county and local governments, and privately owned critical infrastructure where appropriate and authorized by law.

B. Statewide Shared Services

The most operationally consequential State investment is the shared services model. As of May 2026, the State has deployed Endpoint Detection and Response (EDR) coverage on 102,806 endpoints and Attack Surface Management (ASM) across 105,725 assets in county and local government systems across New York. Additionally, utilizing State and Local Cybersecurity Grant Program (SLCGP) funding, the State is distributing more than 112,000 Multi-Factor Authentication (MFA) hard tokens to more than 160 eligible local government entities, school districts, and public authorities to secure identity access management. The savings to county and local governments over a three-year period is over $19 million – money that small jurisdictions, which would otherwise have no realistic path to enterprise-grade cyber tooling, can instead direct to essential services. Beyond the financial savings, the benefit of bringing these entities under the state’s umbrella to improve our whole-of-state cyber posture is invaluable.

The model produces results at every level of the defensive stack. In a single 30-day window in 2025, the EDR shared service identified and remediated 1,178 incidents across New York government entities, 509 of them categorized as high severity, 9 as critical, and 40 requiring human intervention. Over the same period, the State's proactive threat-hunting layer, which operates continuously around the clock, surfaced 28 distinct detections, of which 24 required further investigation. More than a dozen were adversary-in-the-middle attacks on state and local users, sophisticated session-hijacking operations of the type that, three years ago, were almost exclusively the province of well-resourced criminal groups and nation-state adversaries.

The most consequential measure of the program's effect is the one local government leaders care about most. Ransomware incidents reported to the State have declined from 14 in 2023, the year the shared-services investment began, to zero through the

first four months of 2026. This drop, despite increased reporting volume, is the strongest available evidence that investment in shared, state-level cyber defense generates significant returns.

Two operational examples illustrate the difference the shared-services model makes when an intrusion is actually underway. In 2024, the managed EDR service identified a malicious payload associated with a command-and-control framework on a county host following a user's interaction with a fraudulent government form. Detection, containment, and confirmed remediation took 37 minutes. A comparable hands-on-keyboard intrusion in the same period at a county without the managed EDR service took approximately 2,880 minutes, or two full days, to remediate. That difference can be what separates an incident from a crisis.

C. The Joint Security Operations Center and State Cyber Response Teams

New York operates one of the most robust state-level cybersecurity operations centers in the country. The Joint Security Operations Center, operated by the Office of Information Technology Services (ITS), supports State and local government missions 24/7/365. It ingests over 400 terabytes of data per month and processes approximately 350,000 security events per second. In 2025, the Joint Security Operations Center conducted more than 16,000 investigations leveraging over 24,000 detected events; expanded detection capabilities by 92 percent across 41 active use cases; and grew its staff by 33 percent to 65 analysts. The same year, ITS established a new partnership with the New York State Division of Military and Naval Affairs where State active-duty national guardsmen support the Joint Security Operations Center operations full-time in State Active Duty status.

D. Mandatory Cybersecurity Incident Reporting

New York requires municipal corporations and public authorities to report cybersecurity incidents to the Division of Homeland Security and Emergency Services within 72 hours, and to report any ransomware payments within 24 hours.[14] As of May 8, 2026, the State has received 202 mandatory reports. The reporting framework gives the State,

[14] https://www.governor.ny.gov/news/governor-hochul-announces-legislation-now-effect-strengthen-cyberscurity-across-new-york

for the first time, a real-time picture of the threats facing local government, and gives local governments a single coordinated channel for assistance. The reporting framework also enables critical cross-system defense: when a local government reports an account compromise or ransomware indicator, the State can identify accounts used by the affected entity, take precautionary action to reduce spillover risk to State systems, ensure timely and anonymized distribution of indicators of compromises to stakeholders, and ensure that an appropriate law enforcement response is undertaken.

Across State systems, ITS responded to 132 cyber incidents in 2025, a 45 percent increase since 2024. Across local government systems, the Cyber Incident Response Team (CIRT) within the Division of Homeland Security and Emergency Services responded to 145 incidents in 2025 and 157 incidents in the 2026 calendar year through May 8, 2026. The growth in CIRT reporting volume reflects both an expanding threat surface and improving reporting fidelity from a mandatory reporting framework that did not exist eighteen months ago. New York State has continued to grow its law enforcement capabilities as well, including an additional $7.4 million to expand the New York State Police's Cyber Analysis Unit, Computer Crimes Unit and Internet Crimes Against Children Center.[15]

E. Frontier Technology

New York has moved aggressively to address emerging technology threats that federal action has not yet caught up to. In June 2025, Governor Hochul signed the Responsible AI Safety and Education (RAISE) Act, one of the country's first state-level safety frameworks for frontier AI developers.[16] The RAISE Act requires large developers to conduct cyber capability evaluations of frontier models prior to deployment. It requires those developers to report when they detect their models being used in cyber operations against critical infrastructure. And it requires reporting when a developer's model materially contributes to a catastrophic-risk event, defined in statute as a single incident causing more than fifty deaths or serious injuries or more than one billion dollars in damages, where the model provided expert-level assistance in creating a

[15] https://www.governor.ny.gov/news/governor-hochul-announces-nation-leading-cybersecurity-strategy
[16] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20251222

weapon of mass destruction, engaged in unsupervised cyberattack or serious criminal conduct, or evaded developer or user control.

III. RECOMMENDATIONS TO THE SUBCOMMITTEE

The State's experience yields six specific recommendations for consideration by this subcommittee and your colleagues in Congress.

1. Reauthorize and Fully Fund the State and Local Government Cybersecurity Grant Program via the PILLAR Act

The State and Local Cybersecurity Grant Program (SLCGP) is the single most consequential federal investment in the cyber protection of municipal services, public utilities, school districts, and State and local governments in this country. Without reauthorization via the PILLAR Act, the consequences for state and local cyber defense will be immediate and severe. Programs that states have built up over three years cannot be sustained at current scale without more financial support. And in a meaningful number of cases, programs initiated with SLCGP funding will simply shut down, taking the cybersecurity posture of the jurisdictions they serve with them. The PILLAR Act should be the floor, and the program should be robustly funded for the long term.

Four operational adjustments would meaningfully improve the program at reauthorization:

1. The cost-share match requirement is difficult for cash-strapped state and local jurisdictions, and disproportionately burdens the smaller jurisdictions for which the program is most critical. Elimination or substantial reduction of the match should be considered.
2. Funding should be reauthorized at a consistent multi-year level so that states can plan multi-year procurements, vendor relationships, and shared-services contracts against a stable horizon. State input on program priorities prior to release of funding would also improve operational fit, especially to make it easier to engage in software-as-a-service, multi-year, statewide shared services.

3. The current rural/urban percentage allocation structure should be removed or adjusted as it makes it difficult for states to procure sophisticated shared services that benefit all jurisdictions. Removal of these percentage requirements, or a substantial mitigation of them for shared services available for all, would allow states to deploy modern enterprise-grade tooling across mixed-jurisdiction portfolios.
4. Current restrictions that prevent SLCGP funds from being used to purchase Multi-State Information Sharing and Analysis Center (MS-ISAC) memberships and services should be removed. This restriction is contrary to the program's stated purpose. The MS-ISAC, operated by the nonprofit Center for Internet Security, provides nationally sourced threat intelligence, incident response support, and competitively priced cybersecurity tooling to public sector entities at a scale no individual state can replicate cost-effectively. A statewide MS-ISAC membership is among the highest-leverage uses of SLCGP dollars available, particularly for more than 20,000 SLCGP-eligible entities in New York alone, the majority of which are small, rural, or under-resourced jurisdictions.

2. End the Two-Tiered Defense in Artificial Intelligence Access

Frontier AI is collapsing the time between vulnerability discovery and exploitation. State and local governments protect the power grid, the drinking water supply, public health systems, school districts, insurance, and the everyday operations of government. These systems provide more direct services to more Americans than the federal systems for which advanced defensive AI tooling is currently being scoped. Yet state and local cyber defenders have limited structured pathways to the same class of frontier AI capabilities that federal partners and a small number of large enterprises are beginning to access.

The need to address this access gap extends across all levels of government and across both parties. On May 13, 2026 a bipartisan group of thirty-two House members wrote to the National Cyber Director calling for, among other things, "expanded controlled defensive access" to frontier AI for trusted defenders and a framework for managing AI discovered vulnerabilities at scale.[17] This follows a May 4, 2026 joint letter

[17] https://latta.house.gov/uploadedfiles/ai-discovered_vulnerability_coordination_letter.pdf

from 14 states, led by New York,[18] which called for AI companies to better consider and include state, local, and critical infrastructure equities in the development and deployment of their models.

New York is already working with private-sector partners to incorporate frontier AI into its defensive posture. We must establish a structured program through which state fusion centers and state operations centers including New York's JSOC receive priority access to current and future frontier defensive AI capabilities at the same time those capabilities are made available to federal partners and large technology companies.

3. Restore the Federal Government's Capacity to Be a Partner

CISA has lost approximately one-third of its workforce in the past year.[19] The operational consequence in New York is that CISA's availability to State agencies and local governments has materially diminished. The quantity and quality of cyber threat intelligence delivered to states by CISA and the Department's Office of Intelligence and Analysis has declined, including the frequency of classified briefings for cleared personnel.

Congress should resource the CISA workforce to the level the mission now requires.

Six specific items merit congressional attention.

1. CISA should be resourced and authorized to conduct its mission. The cuts to the CISA workforce should be reversed, and CISA should leverage state and regional Fusion Centers as a force multiplier. Fusion Centers maintain the local contacts and trust relationships that allow federal threat reporting to be operationalized at speed. Providing training and dedicated resourcing to Fusion Centers with a cyber component would give CISA proactive reach into communities it currently cannot serve directly.
2. CISA needs consistent, Senate-confirmed leadership to navigate long-term strategic threats and to serve as a stable partner to the states. Acting and vacant

[18] https://www.governor.ny.gov/sites/default/files/2026-05/Joint_Letter_State_Access_Frontier_Models_4MAY2026__.pdf
[19] https://federalnewsnetwork.com/cybersecurity/2026/04/cisa-cyber-partnerships-face-standstill-amid-cuts/

senior roles cannot drive the multi-year coordination required to meet adversaries who operate on a long planning horizon.

3. The Cybersecurity Information Sharing Act of 2015 expires on September 30, 2026. The Act is the legal foundation for the voluntary information sharing among the private sector, the Federal Government, and the states that defend critical infrastructure. Another short lapse will further chill the private-sector reporting that CISA and state cyber operations centers rely on.
4. The Nationwide Cybersecurity Review (NCSR) program has been discontinued. NCSR was a free, annual, anonymous self-assessment tool that local governments used to benchmark cybersecurity maturity against peers, identify gaps, and meet federal grant eligibility requirements, including for SLCGP itself. Its loss creates immediate friction in grant compliance and removes a critical maturity-measurement tool from the field. Restoration of NCSR, or a functional federal equivalent, should be a near-term priority.
5. CISA should complete rulemaking for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and finalize the national reporting framework for critical infrastructure cybersecurity incidents. New York, alongside a group of other states with elected leadership from both parties, provided formal comments on CIRCIA highlighting the importance of federal and state reporting requirements to be harmonized and actionable.[20] The final rule should also include a structured mechanism for CISA to notify state regulators when entities they oversee report covered incidents.
6. CISA should re-establish the Critical Infrastructure Partnership Advisory Council to restore the formal collaborative environment between state and local governments and the private sector. As part of this effort, CISA should designate cloud service providers and major data centers as critical infrastructure, as these environments are critical for state and local governments and critical infrastructure.

4. Establish a Federal Floor for Frontier AI Safety with Reporting Obligations

[20] https://www.regulations.gov/comment/CISA-2022-0010-0458

The Federal Government should establish a regulatory framework for frontier AI development that prevents the proliferation and misuse of cyber-offensive capabilities which threaten homeland security. The framework should be harmonized with the operational requirements of the New York RAISE Act and should include three elements at minimum: pre-deployment cyber-capability evaluations by large developers, with results shared with federal, state, and local stakeholders; mandatory reporting when developers detect their models being used in cyber operations against critical infrastructure; and mandatory reporting of catastrophic-risk events like those defined in the RAISE Act statute.

Federal action of this kind would give industry a single national floor for transparency and safety obligations, and give state and federal defenders the visibility they need to act on emerging risks. It should not, however, preempt state regulation that goes further. States carry the operational consequences of frontier AI deployment most directly, through our critical infrastructure protection, public safety, financial services, and consumer protection authorities. New York's RAISE Act was enacted because federal action has not developed at a pace equal to the evolution of risks. We cannot afford to lose what we have built while waiting for federal action that may or may not come, and that may or may not match the threat.

5. Modernize the Federal Legal Framework for Cyber Prosecutions

Defense and resilience are not sufficient on their own. The Federal Government also must impose consequences on cyber actors, including the transnational criminal organizations that account for the bulk of consequential criminal cyber activity against U.S. targets. Two changes would meaningfully expand that capability.

1. The Cyber Conspiracy Modernization Act,[21] introduced on a bipartisan basis should advance. The bill would allow conspiracy charges under the Computer Fraud and Abuse Act, with penalties scaled to the severity of the underlying conduct. The bill's conspiracy provisions should also be extended to reach those

[21] https://www.rounds.senate.gov/imo/media/doc/cyber_conspiracy_modernization_act.pdf

who knowingly provide or facilitate "bulletproof" hosting infrastructure for cyber crime that enables both criminal and nation-state operators.

2. Federal training programs like the Secret Service's National Computer Forensics Institute[22] provides training for prosecutors on digital evidence and cybercrime. Expanding federal capacity to train law enforcement to investigate these crimes would meaningfully accelerate prosecutor capacity nationwide.

6. Address Cyber Crime on U.S. Infrastructure

The current operating environment enables criminals to spin up cloud computing, purchase infrastructure, and launder cryptocurrency transactions in minutes. Each of these is the product of legitimate U.S. industry. Each is also a force multiplier for fraud, ransomware, account takeover, disinformation, foreign malign influence, and sanction evasion. Pig butchering operations, laptop farms that placed operatives inside dozens of New York-area companies, cyber espionage and attackers, and ransomware crews all rely on the same American-hosted infrastructure to scale.

Frictionless cyber crime on U.S. infrastructure is not an inevitability. It happens on infrastructure that American companies operate and that American law governs. Making that infrastructure harder to reach for our adversaries is one of the most consequential cyber actions Congress can take. Congressional action should focus on three areas.

1. The major cloud and hosting providers should be required to implement and document meaningful know-your-customer and abuse-response practices, with clear federal authority to act when those obligations are not met. The current model relies on voluntary self-regulation that has not kept pace with the threat. A graduated federal framework would create real consequences for providers who knowingly host criminal operations and clear safe harbors for those who do not.
2. Addressing the fraud facilitated by cryptocurrency exchanges requires decisive federal action. The current regulatory gap has allowed predatory scams like pig butchering, sanction evasion, ransomware, and other crimes to flourish at scale. To stop this predictable harm, the Federal Government should implement a

[22] https://www.secretservice.gov/investigations/cyber

national regulatory floor modeled on the New York Department of Financial Services' BitLicense Program, which enforces strict consumer protection, cybersecurity, and capital adequacy requirements.[23] This would help choke off illicit pipelines while maintaining a stable, predictable environment for legitimate crypto enterprises.

3. The Federal Government should accelerate its disruption authorities. The Department of Justice's disruptions of nation-state and cybercriminal groups' cyber operations show that targeted takedowns work when properly resourced.[24, 25, 26] Congress should ensure those authorities, and the cross-agency coordination they require, have the staffing, the funding, and the legal clarity to scale to the current threat environment.

IV. CONCLUSION

Cybersecurity is the silent partner of democracy. When the public utilities, school districts, state agencies, and county governments that constitute the operational fabric of American life are hollowed out by cyberattacks, the institutions that prop up democratic life are hollowed out with them. Reauthorizing the PILLAR Act, restoring federal coordination capacity, opening frontier defensive AI to state defenders, regulating frontier AI development at the federal level without preempting states, modernizing cyber prosecution authorities, and rejecting frictionless cyber crime as a policy default are not six separate items. They represent six elements of a single proposition: that the institutions of self-government in this country are worth defending against threats that do not respect state lines or national borders. Doing so demands the Federal Government to be a partner to all 50 states.

New York is ready to do its part. We want and need the Federal Government as our partner in the work.

---

[23] https://www.dfs.ny.gov/virtual_currency_businesses
[24] https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker
[25] https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-network-controlled
[26] https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal