May 12, 2020

The Honorable James E. Risch
Chairman
Senate Foreign Relations Committee
Dirksen Senate Office Building 423
Washington, DC 20515

The Honorable Bob Menendez
Ranking Member
Senate Foreign Relations Committee
Hart Senate Office Building 528
Washington, DC 20515

Dear Chairman Risch, Ranking Member Menendez, and Members of the Committee:

We, the undersigned civil liberties groups, write to express our opposition to Title IV of S.482, the Defending American Security from Kremlin Aggression Act of 2019.[1] Title IV—titled the International Cybercrime Prevention Act—would unnecessarily expand the Computer Fraud and Abuse Act (CFAA), 18. U.S.C. § 1030, without fixing any of the law's existing problems. The CFAA already threatens beneficial security research, and Title IV, which increases penalties and expands the statute's scope, will only make that threat worse.

Title IV would also create broad new authority for the government to obtain court orders to stop violations of the CFAA, or to order third parties to do so on its behalf. This could result in severe collateral damage, yet Title IV fails to provide any protections and gives users no recourse if their systems are harmed.

We stand strongly opposed to Title IV of S.482 in its current form.

1. **Title IV Unnecessarily Expands the CFAA Without Fixing Any of the Law's Existing Problems.**

Title IV of S.482 would expand the existing prohibition in the CFAA against selling passwords to include any "means of access." Such an expansion is unnecessary and misguided.

First, other criminal statutes already address fraud in connection with access devices.[2] The government has claimed that this amendment is nonetheless necessary to enable prosecution of those selling or renting of botnets to malicious actors, but any such behavior currently constitutes conspiracy to commit a violation of the CFAA. And the CFAA's prohibitions on unauthorized access already criminalize the creation and use of malicious botnets.

---

[1] This coalition letter is limited to Title IV of S.482 and may not represent the undersigned groups' full concerns with regard to S.482 in its entirety.

[2] *See* 18 U.S.C. § 1029.

Second, Title IV's broad language—"means of access"—is in no way limited to the sale or rental of malicious botnets. Significantly, the bill fails to define "means of access." With no guidance, it is unclear how broadly prosecutors or courts will apply this provision. The provision could make criminals of paid researchers who test access in order to identify, disclose, and fix vulnerabilities.

Title IV would also create a broad new criminal violation and harsh penalties for damaging "critical infrastructure" computers. The scope of critical infrastructure has been broadly interpreted by the Department of Homeland Security,[3] which means these harsh penalties could have far-reaching implications—including for the security research community. And, because hacking computers is already illegal under the CFAA, this proposal—and its corresponding threat to beneficial security research—is wholly unnecessary.

Title IV's proposed expansion of the CFAA is not only unnecessary and misguided, but it would make the CFAA much worse. The proposed changes increase penalties, expand the state's scope, and threaten the security community—all while failing to address ambiguity in existing law that has chilled security research, resulted in disproportionate penalties, and criminalized ordinary Internet activity. Title IV would exacerbate the CFAA's existing problems and enable prosecution and civil lawsuits based on behavior well beyond what the CFAA was meant to target: malicious computer break-ins.

In a world where everyone relies on the Internet for their personal and professional lives, Congress should be doing all it can to encourage good faith security research, which helps keep us all safe. Title IV would do the opposite.

2. Title IV Creates New Authority for the Government to Obtain Civil Injunctions to Stop Violations of the CFAA But Fails to Provide Any Protections to Avoid Collateral Damage.

Title IV would also amend 18 U.S.C. § 1345 to give the government new authority to obtain civil injunctions to force companies to stop service, redirect domain names, or take any other actions deemed necessary to stop violations of the CFAA. Though the provision is ostensibly directed at stopping botnets, it could apply to a range of unrelated activities—such as activists who send faxes *en masse* to hundreds of members of Congress at once.

---

[3] The Department of Homeland Security has identified 16 critical infrastructure sectors, including the Information Technology Sector, which it defines as companies that "produce and provide hardware, software, and information technology systems and services, and—in collaboration with the Communications Sector—the Internet." *See* https://www.cisa.gov/information-technology-sector.

Significantly, Title IV fails to require that the government provide notice to innocent consumers who might get caught up in such takeovers, such as botnet victims, or even people who simply use the same services as botnet operators. Millions of Internet users witnessed the damage such lack of notice can cause back in 2014, when Microsoft's attempt to stop an 18,000-node botnet resulted in termination of Domain Name Service (DNS) to nearly 5,000,000 innocent subdomains—all because Microsoft got an *ex parte* court order that blocked notice to the DNS provider, No-IP.com.[4] Had the DNS provider received notice, it could have worked with Microsoft to avoid shutting off service for millions of innocent subdomains that were not a part of the botnet.

Title IV also provides innocent users no recourse if their systems are harmed, and allows companies that assist the government a free pass for any damage caused.

— — —

We urge you to oppose this dangerous and misguided proposal. If you have any questions, please contact India McKinney at india@eff.org or 415-436-9333.

Sincerely,

American Civil Liberties Union
Center for Democracy and Technology
Copia Institute
Defending Rights & Dissent
Demand Progress
Electronic Frontier Foundation
National Association of Criminal Defense Lawyers
New America's Open Technology Institute
Restore the Fourth
The X Lab

[4] Nate Cardozo, 'What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business,' Deeplinks (July 10, 2014) https://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking.