

POLITICO



POLITICO



POLITICO

Weekly Cybersecurity

Delivered every Monday by 10 a.m., Weekly Cybersecurity examines the latest news in cybersecurity policy and politics.

✉ **re Weekly Cybersecurity newsletter**

By signing up you agree to receive email newsletters or updates from POLITICO and you agree to our privacy policy and terms of service. You can unsubscribe at any time and you can contact us here. This sign-up form is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

New DoD vulnerability effort launched

By **MARTIN MATISHAK** | 04/05/2021 10:00 AM EDT

Editor's Note: Weekly Cybersecurity is a weekly version of POLITICO Pro's daily Cybersecurity policy newsletter, Morning Cybersecurity. POLITICO Pro is a policy intelligence platform that combines the news you need with tools you can use to take action on the day's biggest stories. Act on the news with POLITICO Pro.

QUICK FIX

- **EXCLUSIVE: The Defense Department and HackerOne today kickoff a pilot program to root out digital weaknesses in the sprawling defense industrial base.**
- **An influential tech group has recommendations for how the U.S. can tackle its semiconductor supply chain woes.**
- **President Joe Biden's pick for the Pentagon's top intel job has some cyber chops.**

HAPPY MONDAY and welcome to Morning Cybersecurity! Send your thoughts, feedback and especially tips to mmatishak@politico.com. Be sure to follow [@POLITICOPro](https://twitter.com/POLITICOPro) and [@MorningCybersec](https://twitter.com/MorningCybersec). Full team info below.

FIRST IN MC: A LITTLE DIB'LL DO YA — The Pentagon's Cyber Crime Center and bug bounty vendor HackerOne today launched an effort to share vulnerability data and boost digital hygiene within the defense industrial base, a frequent target for hackers that has been rocked by a number of high-profile breaches over the years. The Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot — started in collaboration with the Defense Counterintelligence and Security Agency — will invite security researchers to hunt for vulnerabilities in more than 100 DIB assets across several different organizations.

The 12-month program aims to apply the lessons learned from the existing 28,000 reports made through the Pentagon's Vulnerability Disclosure Program, which was established in 2016, to vendors and contractors within the DIB. The pilot program's structure was informed by the Carnegie Mellon University's Software Engineering Institute, which conducted a feasibility study ahead of the initiative.

“To have a comprehensive view of where you're most vulnerable in order to protect against evolving threats, you need to remain open to vulnerability findings at all times. It's a best practice and a regulatory expectation,” HackerOne Co-founder Michiel Prins said in a statement. “With the DIB VDP, learnings from this best-in-class program can be extended to many of the government's most vital suppliers.”

INDUSTRY INTEL

© 2021 POLITICO LLC