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 and @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

CALL AND RESPONSE — The federal government should boost its semiconductor industry through a variety of tax incentives, trade protection and regulatory changes, according to the Information Technology Industry Council. The various suggestions come in response to the Commerce Department's recent call for feedback on the state of the semiconductor manufacturing industry. "While ITI represents the breadth of the technology sector and counts several leading global semiconductor manufacturers amongst our membership, our response is informed by an end-user perspective on the importance of semiconductors to our industry," the group wrote.

The council offers the government a series of recommendations on how to strengthen American leadership in a space where it's been lagging behind. It suggests providing incentives to enhance the U.S. semiconductor industry through funding for the bipartisan CHIPS for America Act and for refundable investment tax credits for all multinational chip manufacturers that meet the required standards and guidelines; tackling unfair Chinese trade practices; expanding access to global markets for U.S. semiconductor research and development; and bolstering the tech workforce through STEM education efforts and immigration reforms.

PENTAGON

PENTAGON INTEL CHIEF PICKED — President Biden on Friday announced that he would tap U.S. intelligence community veteran Ronald Moultrie to be undersecretary of defense for intelligence and security. Moultrie previously held roles with the CIA and the Office of the Director of National Intelligence. He retired in 2015 as the NSA's director of operations.

Moultrie also helped author the Cybersecurity Readiness Review for the U.S. Navy, commissioned by former Secretary Richard Spencer, which found that the service's failure to properly secure its IT systems represented an "existential threat" to both its survival and that of the Marine Corps. The review also found that of the Nay's leaders understood the magnitude of the challenge. Moultrie is the president and chief executive of Oceanus Security Strategies and was a member of the Biden-Harris transition team for the intelligence community.

HACKED

MORE VULNERABILITIES TO FIX — The FBI and CISA on Friday warned that hackers are exploiting previously known vulnerabilities in Fortinet software to gain access to government and industry networks. "The APT actors may be using any or all of these CVEs to gain access to networks across multiple critical infrastructure sectors to gain access to key networks as pre-positioning for follow-on data exfiltration or data encryption attacks," the organizations said in an advisory.

The bulletin cites three known vulnerabilities in Fortinet's FortiOS that have been identified over the last three years and recommends organizations using the software to immediately patch them. "APT actors may use other CVEs or common exploitation techniques—

such as spearphishing—to gain access to critical infrastructure networks to pre-position for follow-on attacks," the advisory warned, noting hackers have "historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns."

EDUCATION DEPARTMENT

SCHOOLHOUSE CYBER — Democratic Reps. Doris Matsui(Calif.) and Jim Langevin (R.I.) on Friday requested the Education Department to allow schools to invest more money in cybersecurity. "While the shift to online interaction has helped keep students engaged, it has also highlighted a growing threat — cyber-incidents targeting schools that are increasing in regularity and sophistication," the pair wrote in a letter to Education Secretary Miguel Cardona.

"To help ensure schools are keeping pace with the demands of the modern classroom, we urge you to issue guidance that will allow K-12 schools to make needed investments in increased cybersecurity measures," they added.

Matsui and Langevin urged Cardona to issue guidance clarifying that funds included in recent Covid-19 relief packages for K-12 institutions can also be used to boost cybersecurity. "While schools can reasonably interpret this text to indicate cybersecurity costs would be considered eligible expenses, written guidance from the Department to that effect will ensure schools have the information they need to make informed decisions about how to use these funds," they wrote.

QUICK BYTES

— CISA's top lawyer lays out what considerations should go into a cybersecurity legal practice.

— How DHS 'threat hunters' became prey themselves.

— The manufacturing sector has a ransomware problem it doesn't want to talk about.

— The personal information for over 500 million Facebook users has been found on a hacking website.

That's all for today.

Stay in touch with the whole team: Eric Geller (egeller@politico.com,@ericgeller); Bob King (bking@politico.com,@bkingdc); Martin Matishak (mmatishak@politico.com, @martinmatishak); and Heidi Vogt (hvogt@politico.com,@heidivogt).

Follow us on Twitter

Heidi Vogt @HeidiVogt
Maggie Miller @magmill95
John Sakellariadis @johnnysaks130

FOLLOW US

Careers

Credit Card Payments

Digital Edition

FAQ

Feedback

Headlines

Photos

POWERJobs

Press

Print Subscriptions

Request A Correction

Write For Us

RSS

Site Map

Terms of Service

Privacy Policy

Do not sell my info

Notice to California Residents