POLITICO
Morning Cybersecurity
A daily briefing on politics and cybersecurity

DHS highlights progress on DNS tampering prevention efforts

By TIM STARKS (tstarks@politico.com; @timstarks)02/15/2019 10:00 AM EST

With help from Eric Geller and Martin Matishak

Programming note: *Morning Cybersecurity will not publish on Monday. Our next Morning Cybersecurity newsletter will publish on Tuesday.*

Editor's Note: This edition of Morning Cybersecurity is published weekdays at 10 a.m. POLITICO Pro Cybersecurity subscribers hold exclusive early access to the newsletter each morning at 6 a.m. To learn more about POLITICO Pro's comprehensive policy intelligence coverage, policy tools and services, click here.

QUICK FIX

— Most federal agencies have completed tasks that DHS ordered to head off domain name infrastructure tampering, a top official said. But some have failed to meet the deadline.

— The NSA and Cyber Command chief wants to be more public about some of its work. Namely, he says it's beneficial to share some details about the agency's election security efforts, past and present.

— A top Republican said House Democrats' election bill has more worrisome provisions for cybersecurity. The overall legislation, he said, makes the U.S. vulnerable.

HAPPY FRIDAY and welcome to Morning Cybersecurity! Hope you had a Happy Valen-... oh. Send your thoughts, feedback and especially tips to tstarks@politico.com, and be sure to follow @POLITICOPro and @MorningCybersec. Full team info below.

DRIVING THE DAY

DNS, AND MY DOGS BITE — Federal civilian agencies are approximately 75 percent of the way toward completing mandates that the DHS Cybersecurity and Infrastructure Security Agency established in its first emergency order to prevent a domain name hijacking campaign, agency director Chris Krebs told MC on Thursday. Issued on Jan. 22 during the partial government shutdown, the order gave agencies four steps to combat Domain Name System infrastructure tampering that would allow attackers to redirect and intercept web and email traffic — and gave them 10 business days to do so.

Despite some agencies missing that deadline — which, as Krebs acknowledged, was made more difficult by the shutdown — he said he was happy with the results so far. "Across the four actions, we're pretty satisfied with the response rate," Krebs said. "There are some micro agencies having some challenges. That's where we come in as a service to help work them through and put them on a plan." What's proven most difficult, he said, is the demand that agencies implement multi-factor authentication for DNS accounts, because many agencies have "outsourced DNS record management to a provider who can't implement MFA, technically."

The emergency directive appears to have inspired those outside the federal government, too, with Krebs saying he heard from a major metropolitan area that it would adopt the guidance as well. He said he has seen that with other DHS directives, with the department viewed by others outside the federal government as a "credible, authoritative voice" sending the message that "this is a risk and you need to work on it." In the same interview, Krebs criticized a story saying DHS had downgraded election security task forces. Look for more from Tim's sitdown with Krebs soon.

BUDGET

CISA BUDGET BE LIKE — A newly approved compromise funding package would devote $1.68 billion to CISA, according to Senate appropriators, a reduction from last year because the Office of Biometric Identity Management moved to another part of DHS. POLITICO's Mary Lee has most of the details across multiple agencies here.

A $33 million infusion for the DHS Election Infrastructure Security Initiative, a boost from last year's $26.2 million, would "build out incident response, our ability to do exercises, risk and vulnerability assessments, remote penetration testing, training to local jurisdiction" and other functions, Krebs told reporters Thursday in a conference call. The Secret Service would also get an extra $6 million to train state and local officials on cybercrime investigations.

SHH! IT'S A SECRET — U.S. Cyber Command and NSA chief Army Gen. Paul Nakasone on Thursday committed to publicly sharing more details about how his organizations helped defend last year's midterms from foreign interference. "The success that we had in 2018, more of our nation should know about," Nakasone told the Senate Armed Services Committee. Nakasone — who predicted Cyber Command would grow as digital adversaries evolve — said the whole-of-government

Nakasone also committed to informing the public more about malicious digital threats ahead of the 2020 election. “Being able to educate the public is critical for us,” the four-star said. His comments were welcomed by panels members on both sides of the aisle. “The enemies know what they’re doing, we know what they’re doing, to some extent, they know we know what they’re doing. The only ones who are in the dark, really, are the American people,” said Sen. Richard Blumenthal.

H.R. 1 AND ITS DISCONTENTS — House Democrats’ push to impose new election security standards on states through their marquee election bill (H.R. 1) would undermine cybersecurity, according to the top Republican on the House Administration Committee. “It’s a bill that would nationalize and federalize our election process, which, in my opinion, would make it easier for nefarious groups or even nation-states to try and affect our electoral process,” Rep. Rodney Davis told reporters Thursday after speaking at a Bipartisan Policy Center event on election administration. Davis also blasted the bill hours earlier during a committee hearing.

Davis didn’t say what kinds of federal standards he considered appropriate but warned that “any mandate coming from the federal government” needed accompanying funding. Davis, whose Illinois district includes many rural communities, said a law that required certain voting technology but lacked associated funding “would break many of our local counties.”

Davis likewise declined to say whether he would press House Administration Chairwoman Zoe Lofgren to carve out H.R. 1’s election security provisions into a separate bill. “Chairperson Lofgren and the Democrats on our committee clearly are pushing this comprehensive approach rather than an individual approach,” he said. Democrats have denied the bill attempts to nationalize the election process, but say the federal government has a role because local officials administer national elections, and local officials are ill-equipped to combat nation-state cyberattacks without federal help.

IT’S ELECTRIC — At a Thursday Senate Energy Committee hearing, Federal Energy Regulatory Commission Chairman Neil Chatterjee said his call for mandatory cybersecurity standards for national gas pipelines may no longer be the right approach, with industry and government showing interest in improving the current processes. The top Democrat on the panel, Sen. Joe Manchin, asked how feds could help smaller utilities comply with cybersecurity standards. Sen. Angus King, speaking on the cyber threat to the grid from Russia, said “We’re entirely too calm about this.”

YES, ANOTHER WORKING GROUP — The U.S. and Poland on Thursday announced the creation of four working groups, one focused on cybersecurity, to “drive momentum toward concrete solutions” for problems facing the Middle East. The “Combating Cyber and Emerging Threats” working group will deal with both cybersecurity and energy security issues. The Middle East is a hotbed of malicious cyber activity, much of it focused on the energy sector, with the 2012 Saudi Aramco hack being the most famous example.

The new working groups were born at a meeting of foreign ministers from 62 countries in Warsaw this week where officials discussed, among other things, “combating threats to cyber and energy infrastructure.” According to a joint readout from the U.S. and Poland, “Many of the participating countries expressed an intention to continue to act collaboratively to promote a more prosperous future for the region and its people,” which led to the creation of the working groups.

TWEET OF THE DAY — Evocative.

PEOPLE ON THE MOVE

— From our friends at Patent Politics: Henry “Jamie” Holcombe has been appointed U.S. Patent and Trade Office chief information officer, the agency announced Wednesday.

QUICK BYTES

— Cyber pro association (ISC)^2 announced a Professional Development Institute.

— George Washington Unversity’s National Security Archive looked at a Russian social media campaign during the Charlottesville, Va., rallies.

— How Ukrainian political operatives weaponized Tinder, via the Joseph Rainey Center for Public Policy.

— WannaCry fighter and accused malware creator Marcus Hutchins lost a bid to rule out comments he made after partying at DEF CON. Ars Technica

— The controversial NSO Group was sold. Globes

— “Software pirates use Apple tech to put hacked apps on iPhones.” Reuters

— A couple Atlantic Centerers examine the difficulty of joint cyber attribution. Lawfare

— "Amazon's Home Surveillance Chief Declared War on 'Dirtbag Criminals' As Company Got Closer to Police." Intercept

That’s all for today. No but seriou-... oh.

Stay in touch with the whole team: Mike Farrell (mfarrell@politico.com, @mikebfarrell); Eric Geller (egeller@politico.com, @ericgeller); Martin Matishak (mmatishak@politico.com, @martinmatishak) and Tim Starks (tstarks@politico.com, @timstarks).