

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074
<http://oversight.house.gov>

May 5, 2020

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington D.C. 20535

The Honorable Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington D.C. 20528

Dear Director Wray and Director Krebs:

I am writing to request a briefing for Members of the Subcommittee on National Security on the growing and alarming number of cyberattacks that are threatening U.S. federal government departments and agencies, international organizations, and private entities during the coronavirus pandemic.

Since the beginning of the global health crisis, malicious cyber actors—some of whom may have connections to China, Russia, and Iran—reportedly have sought to exploit the coronavirus crisis to gain a national security advantage over the United States:

- On March 16, 2020, a cyberattack targeted the computer systems of the Department of Health and Human Services (HHS) in an apparent attempt to disrupt the Department's response to the coronavirus crisis.¹
- On April 2, 2020, Reuters reported that hackers associated with Iran had targeted the personal email accounts of World Health Organization (WHO) personnel.² Almost three weeks later, the SITE Intelligence Group reported that nearly 25,000

¹ *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*, Bloomberg (Mar. 16, 2020) (online at www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response).

² *Exclusive: Hackers Linked to Iran Target WHO Staff Emails During Coronavirus*, Reuters (Apr. 2, 2020) (online at www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC).

email addresses and passwords from the WHO, the National Institute of Health, and the Bill and Melinda Gates Foundation had been posted online by unknown actors in an attempt to harass those responding to the virus.³

- On April 8, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom’s National Cyber Security Centre issued a joint alert assessing that advanced persistent threat groups and cybercriminals “are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months” through phishing campaigns, malware distribution, the registration of new domain names, and attacks against remote access and teleworking systems.⁴
- On April 13, 2020, the Department of Defense said it was monitoring a “surge of spear phishing related to COVID-19” and emerging cybersecurity incidents due to higher numbers of personnel teleworking from home.⁵
- On April 15, 2020, the FBI and Secret Service issued a press release which stated: “[S]cammers are targeting websites and mobile apps designed to track the spread of COVID-19 and using them to implant malware to steal financial and personal data. Thieves are even posing as national and global health authorities, including the U.S. Centers for Disease Control and Prevention and the World Health Organization, to conduct phishing campaigns.”⁶
- On April 16, 2020, the Deputy Assistant Director of the Federal Bureau of Investigation’s Internet Crime Complaint Center (IC3) told a webinar audience that IC3 had seen a nearly fourfold increase in reported cyber-crime since the beginning of the coronavirus pandemic, stating: “Countries have a very high interest in information on the virus ... such as information on a vaccine. ... We have certainly seen reconnaissance activity and some intrusions into some of

³ *Nearly 25,000 Email Addresses and Passwords Allegedly From NIH, WHO, Gates Foundation and Others are Dumped Online*, Washington Post (Apr. 22, 2020) (online at www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/).

⁴ Cybersecurity and Infrastructure Security Agency, *COVID-19 Exploited by Malicious Cyber Actors* (Apr. 8, 2020) (online at www.us-cert.gov/ncas/alerts/aa20-099a).

⁵ Department of Defense, *Defense Department CIO and Joint Staff CIO Brief Reporters on DOD Communication Efforts Regarding COVID-19* (Apr. 13, 2020) (online at www.defense.gov/Newsroom/Transcripts/Transcript/Article/2147989/defense-department-cio-and-joint-staff-cio-brief-reporters-on-dod-communication/).

⁶ Federal Bureau of Investigation, *FBI and Secret Service Working Against COVID-19 Threats* (Apr. 15, 2020) (online at www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats).

those institutions, especially those who have identified themselves as working on COVID research.”⁷

- On April 22, 2020, the Google Threat Analysis Group published findings that government-backed hackers, while unsuccessful, had sought to target the personal accounts of U.S. government employees with “phishing lures using American fast food franchises and COVID-19 messaging.”⁸

As the United States continues to grapple with the coronavirus crisis, malicious attempts to compromise U.S. and international information technology systems could undermine the global public health response and threaten U.S. geopolitical interests.

Given these risks, I respectfully request that you provide a briefing to Members of the Subcommittee on National Security by May 22, 2020, to address the following questions:

1. Which federal government departments or agencies involved in the U.S. coronavirus response are the primary targets for malicious cyber actors?
2. Who are the primary actors responsible for the cyber-incidents targeting these agencies and departments? With what level of confidence can the FBI or CISA assess that these attacks are state-sponsored or government-backed?
3. What are the primary objectives of these attacks? How many of these attacks have been successful?
4. To what extent are the same actors targeting the U.S. healthcare system? Are the objectives of these cyberattacks the same or different from those targeting federal government departments and agencies?
5. What observable trends or patterns have the FBI or CISA discerned related to cyberattacks against the U.S. healthcare system? What steps have been taken to inform local hospitals and research facilities of this growing threat from cyberattacks?
6. What steps are the FBI and CISA taking to reinforce the security of local hospitals’ information technology systems? What are the greatest weaknesses, vulnerabilities, and challenges in doing so?

⁷ *FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic*, The Hill (Apr. 16, 2020) (online at <https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic>)

⁸ *Findings on COVID-19 and Online Security Threats*, Google Threat Analysis Group (Apr. 22, 2020) (online at <https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/>).

The Honorable Christopher A. Wray

The Honorable Christopher C. Krebs


Page 4

7. How are the FBI and CISA working with international partners to share information and best practices about these cyber-incidents?
8. How are the FBI, CISA, and other federal entities, such as U.S. Cyber Command, counteracting these attacks and working to deter future incidents?

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

Thank you for your urgent attention to this matter. If you have any questions regarding this request, please contact Subcommittee staff at (202) 225-5051.

Sincerely,



Stephen F. Lynch

Chairman

Subcommittee on National Security

cc: The Honorable Glenn Grothman, Ranking Member