EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF THE NATIONAL CYBER DIRECTOR
WASHINGTON, D.C. 20503

January 20, 2022

The Honorable Carolyn B. Maloney
Chairwoman, Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairwoman Maloney:

Thank you for the opportunity to testify before the Committee on Oversight and Reform. Enclosed are my responses to the questions submitted for the official record following the hearing on Tuesday, November 16, 2021, titled "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats."

For any follow up questions, please reach out to the Office of the National Cyber Director Executive Secretary, Caroline Chang.

Sincerely,

Chris Inglis
National Cyber Director

Enclosure

cc: The Honorable James Comer, Ranking Member

Responses for the Honorable Carolyn B. Maloney

Chairwoman, Committee on Oversight and Reform

Responses from Director Chris Inglis

National Cyber Director, Executive Office of the President

November 16, 2021, Hearing: "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"

---

1. *You have previously testified that there has been a discernible decrease in ransomware attacks from Russian-based groups. However, Assistant Director Vorndran testified that the FBI has not seen a decrease in ransomware attacks in the past couple months originating from Russia. Can you clarify your previous comments regarding the discernible decrease in ransomware attacks?*

   USG officials are on the same page: we have seen reports that some criminal groups have shut down or reduced their activity, and we are pleased that we have not seen additional attacks of the size and consequence of earlier this year, yet ransomware remains at unacceptable levels. We are going to keep bringing the power and capacity of the United States government to bear to disrupt these criminals, their financial enablers, and their infrastructure. We also welcome reports that the Kremlin is taking law enforcement steps to address ransomware emanating from its borders with the recent arrest of several ransomware actors.

   I would also note that baselining ransomware incidents is hard because unless a victim comes forward, the U.S. government does not see most incidents. Currently, the best insights regarding ransomware incidents often come from private sector entities who monitor public and private networks to block attacks. This highlights the need for mandatory reporting of ransomware and other cyber incidents by the private sector, which the Administration supports.

2. *Despite the Administration's successes in raising the profile of ransomware attacks among our allies, two countries stand out in terms of their longstanding unwillingness to tackle ransomware: Russia and China. How can we encourage these countries to cooperate on law enforcement matters? How should the United States respond if they do not take action in response to public indictments?*

The Administration is committed to bringing the full weight of U.S. government capabilities to disrupt ransomware actors, networks, financial infrastructure, and other facilitators. Denying ransomware actors safe haven and holding them accountable are marks of responsible state behavior in cyberspace. The United States and our allies and partners are committed to ensuring that responsible behavior like this is expected of one another by the international community, that norms consistent with responsible behavior are strengthened and incentivized, and that irresponsible behavior brings cost. This commitment with a wide array of international partners was demonstrated in the joint statement with over 30 nations that came out from the White House-led Counter-Ransomware Initiative. We are also taking steps internationally to ensure that anti-money laundering and countering financing of terrorism (AML/CFT) controls are strengthened worldwide for virtual currency exchanges consistent with the standards of the Financial Action Task Force (FATF) to help isolate ransomware actors from their ability to monetize their activities, and we are in discussions with those few jurisdictions where such actors may still find sanctuary.

The President believes in diplomacy. President Biden and President Putin set up a White House-Kremlin experts group on ransomware last June. We welcome reports that the Kremlin is taking law enforcement steps to address ransomware emanating from its borders with the recent arrest of several ransomware actors. We are committed to seeing those conducting ransomware attacks against Americans brought to justice, including those that conducted attacks on JBS, Colonial Pipeline, and Kaseya. As the President has said, cyber criminals are resilient, and we will continue to take action to disrupt and deter them while engaging in diplomacy, with Russia and with allies and partners around the world.

3. *During your confirmation hearings before the Senate, you stated that your position would "create coherence" among federal agencies on cybersecurity. How are you ensuring our cyber strategy includes and represents all federal agencies that may experience, or oversee an industry that experiences, a cyber-attack?*

ONCD is in discussions with senior leadership across the United States Government, learning about how disparate agencies and stakeholders approach shared challenges, how they engage with industry, and where priorities overlap or diverge. We are working arm-in-arm with CISA and other SRMAs to ensure our national strategies are posturing us to overcome seams in organizations and authorities, to respond to cyber incidents with speed and shared insight, and to learn from those incidents in order to build an ecosystem that is resilient and defensible against such incidents over the long term. Federal CISO Chris DeRusha is also serving as a Deputy National Cyber Director to ensure coherence

on Federal Civilian Executive Branch cybersecurity. I have personally met with 18 Federal CISOs as I canvass departments and agencies to understand their challenges.

4. *What can the Administration and Congress do to make cryptocurrency less attractive to cybercriminals?*

   The Administration is taking significant action to combat the misuse of cryptocurrency in support of ransomware activities, which is one of our four priority lines of effort in our counter-ransomware approach. Effective regulation and enforcement activities are key elements of our approach to make cryptocurrencies less attractive to cybercriminals.

   The Department of the Treasury has been at the forefront of this issue for many years, and we are continuing to build on their work through efforts to drive international implementation of standards for virtual asset service providers, explain risks and typologies of ransomware payments and associated money laundering typologies to financial institutions, and take action to disrupt illicit actors using cryptocurrency to support ransomware activity. In 2021, the Office of Foreign Assets Control designated cryptocurrency exchanges SUEX OTC, S.R.O., and Chatex, and associated support networks, for their part facilitating ransomware payments. OFAC also announced updated guidance around ransomware payments, as well as sanctions compliance guidance for cryptocurrency activities, emphasizing U.S. persons' obligations to comply with sanctions obligations and encouraging financial institutions and other companies to work closely with U.S. government agencies like CISA and law enforcement if they are hit with ransomware or asked to help facilitate a ransomware payment.

   Taking law enforcement action against those misusing cryptocurrency or failing to meet their statutory obligations to comply with frameworks like AML/CFT controls are also critical. In October 2020, the Department of Justice published the "Cryptocurrency Enforcement Framework," which was the work of the Attorney General's Cyber Digital Task Force. In October 2021, the Department also stood up a National Cryptocurrency Enforcement Team to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors. While law enforcement organizations and regulators continue to use the authorities available, we need to ensure that investigators and prosecutors have the tools and training that they need to identify illicit cryptocurrency flows and actors and ultimately hold them accountable.

5. *Do we need to be doing more, in terms of regulation or legislation, to make sure that legitimate cryptocurrency exchanges keep criminal proceeds off their platforms?*

The United States has been a leader in regulation and oversight of cryptocurrency activities. Cryptocurrency exchanges operating wholly or in substantial part in the United States are already subject to AML/CFT obligations under the Bank Secrecy Act, administered by the Financial Crimes Enforcement Network (FinCEN). However, the key challenge in combating these illicit activities, which are enabled by the instantaneous cross-border value transfer permitted via cryptocurrencies, is jurisdictional arbitrage. Illicit actors and exchanges "shop around" for jurisdictions that have failed to emplace sufficient AML/CFT regulations and enforcement regimes consistent with the FATF standards. While the regulations related to such exchanges are outside the remit of the ONCD, the White House is very focused on these issues, and we will continue to advocate that all options – including efforts to make it more difficult for criminals to use cryptocurrency exchanges – are considered as part of our holistic government approach to combatting ransomware.

Responses for the Honorable Gerald E. Connolly

Responses from Director Chris Inglis

National Cyber Director, Executive Office of the President

November 16, 2021, Hearing: "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"

---

1. *For over a decade, the Cybersecurity and Infrastructure Security Agency (CISA) has administered a Continuous Diagnostics and Monitoring (CDM) program to help strengthen the cybersecurity of government networks and systems. CDM provides federal agencies with capabilities and tools that find and prioritize risks to federal networks, but not every agency is participating in the CDM program, leaving the National Cyber Director and CISA with potential blind spots across the .gov domain space. In addition, over 80% of critical infrastructure is owned and operated by the private sector, and the Department of Homeland Security has almost no visibility into the security of those operators' networks. Tools like security ratings can provide your office and the Sector Risk Management Agencies with at least some visibility into the cyber hygiene of critical infrastructure operators and industries. How does your office plan to gain visibility into the cyber threat landscape facing critical infrastructure and federal agencies?*

   Gaining greater visibility into the cyber threat landscape facing critical infrastructure and federal agencies is a priority of ONCD. Recent intrusion campaigns demonstrate the need to deepen our visibility into cybersecurity risks and scale our ability to coordinate and respond to cyber incidents.

   This visibility is not gained through a single score card or rating system, but through a multi-pronged approach that involves partnering with the National Security Council, the Office of Management and Budget, the Cybersecurity and Infrastructure Security Agency, Sector Risk Management Agencies, Federal CIOs and CISOs, and private sector partners.

   Increasingly, CISA, FBI, NSA, and SRMAs pool their expertise to produce cybersecurity awareness messages and other bulletins to convey cyber threats and technical indicators to the private sector, so they can take defensive action.
   There are several elements that allow us the visibility into vulnerabilities as well as threats:

- Although historically, the Continuous Diagnostics and Mitigation (CDM) Program has not had the desired level of agency adoption, with the recent executive order and legislative changes, we are seeing an increase in adoption across federal agencies. Currently, 53 agencies are sending data and information to the federal dashboard. There are lines of effort underway within CISA to greatly boost these numbers.

- In addition, OMB Memorandum 22-05, "Guidance on Federal Information Security and Privacy Management Requirements," requires both NIST and CISA to work together to develop a strategy to continue to evolve machine-readable standards for cybersecurity performance and compliance data through CDM (or successor process).

- Federal agencies are now required to implement vulnerability disclosure policies that provide central intake systems for vulnerability reports from the general public, and CISA has created a shared vulnerability disclosure platform for agencies with increasing adoption. These programs have led to more consolidated and centralized tracking of agency vulnerabilities that facilitate greater situational awareness.

- Executive Order 14028 and the federal Zero Trust Strategy are driving initiatives that will increase enterprise-wide visibility into vulnerabilities and attack surface. This includes government-wide adoption of endpoint detection and response (EDR) tools that will be configured to allow CISA access to agency EDR data, and deeper discovery, analysis, and reporting by CISA of agencies' internet-visible assets.

- In addition, existing and evolving partnerships between the federal government and the private sector, such as the Joint Cyber Defense Collaborative, the Sector Coordinating Councils, and others, provide robust fora for the exchange of valuable information and best practices. They also help ensure that the federal government has a window into private sector assets and networks, including critical infrastructure, and vice-versa. We intend to continue strengthening them.