Testimony of National Cyber Director J. Chris Inglis
United States House of Representatives
Committee on Oversight and Reform

November 16, 2021

Chairman Maloney, Ranking Member Comer, distinguished members of the Committee, and your dedicated staff, thank you for the honor to appear before you today alongside Director Easterly from the Cybersecurity and Infrastructure Security Agency (CISA) and Assistant Director Vorndran from the Federal Bureau of Investigation (FBI). It is a privilege to share the witness table with colleagues who lead the cybersecurity work of CISA and FBI. CISA's role as the operational coordinator for federal cybersecurity and support to our Nation's critical infrastructure, combined with FBI's deep expertise and its essential role in victim assistance, investigation, attribution, and threat disruption, comprises a breadth of experience, authority, and resource that makes a critical difference for the American people. Cyber is a team sport, and I couldn't ask for better teammates than Jen and Bryan. We speak on a weekly basis, sometimes even daily, and our staffs are in touch even more frequently. Indeed, both CISA and FBI have been instrumental in providing talent and expertise to help stand up the new Office of the National Cyber Director (ONCD).

I am eager to update you today on the Biden-Harris Administration's continuing actions to counter ransomware and improve our national cybersecurity posture. You can measure the President's commitment to cybersecurity as a critical matter of national security by the positions he has created, the appointments he has made, and the unmatched speed with which the Administration continues to modernize our defenses and bolster our security. That includes recent actions to prevent, deter, and mitigate ransomware attacks against public and private sector networks, as well as efforts to bring ransomware actors to justice.

Before turning to ransomware, allow me to say a few words about the office I have the privilege to lead. I appear before you today as the first National Cyber Director (NCD), a position Congress created just last year, then confirmed me to fill following my nomination by President Biden. I am grateful for the confidence that the President and Congress have placed in me, as well as for the essential investments in cybersecurity and critical infrastructure resilience

that you included in the recently enacted Infrastructure Investment and Jobs Act. I remain committed to engaging with you as we take on these critical, shared imperatives.

To that end, I am pleased to tell you that our new office is making progress as a full-fledged leader in those imperatives. On Thursday, October 28, I released the NCD's first *Strategic Intent Statement*, which outlines the initial strategic approach and scope of work I expect my office to undertake. At the same time, I announced the designation of Chris DeRusha as Deputy National Cyber Director for Federal Cybersecurity, a dual-hatted title he will hold along with his current role as Federal Chief Information Security Officer, creating unity of effort and unity of purpose in our shared mission to ensure the security of Federal systems and networks. Both of these announcements lay the groundwork for the ONCD's approach but are certainly not the sum total of our endeavors. We stand at roughly 20 staff now and will continue to build our team and increase our contributions to the Nation's overall cybersecurity posture with the help of funds included in the Infrastructure Investment and Jobs Act.

Our *Strategic Intent Statement* will soon be followed by a more comprehensive description of our priorities and strategic objectives, which will guide our work for years to come. My office looks to four key outcomes as a benchmark of our success:

- To drive coherence across the Federal cyber enterprise, ensuring that the government is speaking with one voice, moving in the same direction, and, to the greatest extent practicable, sharing common priorities by which we can organize our collective efforts for maximum possible effect;

- To continue to strengthen and improve public-private collaboration in cybersecurity, working closely with CISA, the National Institute of Standards and Technology (NIST), and Sector Risk Management Agencies to expand engagement and partnership across sectoral lines to new levels, including through the new Joint Cyber Defense Collaborative, hosted by CISA;

- To ensure the U.S. government is aligning our cyber resources to our aspirations and accounting for the execution of cyber resources, working closely with the Office of Management and Budget to assess and evaluate the performance of these investments and advising departments and agencies on recommended changes; and

- To increase present and future resilience of technology, people, and doctrine, not only within the Federal government, but also across the American digital ecosystem.

None of this work occurs in a vacuum, and much of the credit for progress in developing these themes and in the work of putting them into practice must go to my partners at the National Security Council, my colleagues sitting alongside me, and many others serving in the Federal cyber ecosystem, which is, of course, inextricably linked to the national cyber ecosystem.

Attempting to subvert that cyber ecosystem is attractive to our adversaries and frustrating to our allies because of how difficult it is for any one country or entity to form a complete picture of actions and actors across its shared spaces. Cyberspace allows a reach and efficiency of scale unrivaled in any other domain, meaning that, employing cyberspace, our geopolitical competitors can have global reach and strategic effect, while criminals and malicious actors can wield an unprecedented level of influence, impact, and coercion. That's especially true when it comes to the scourge of ransomware.

In a nutshell, ransomware is malicious software that infects a computer, or computer network, then encrypts and often steals the data on that system until its owner agrees to pay a ransom for the decryption keys, usually in the form of a virtually untraceable cryptocurrency. A ransomware attack can cripple the enterprise it targets, whether that's a supermarket, a local grain cooperative, a municipal government, or a natural gas pipeline operator. And ransomware actors are becoming both more creative and more malevolent. They have used supply chain operations to target trusted software and managed service providers that support vulnerable small businesses. They have bragged about hacking insurance companies to steal information about which businesses have coverage and will therefore be most willing to pay—and then attacking the insurance companies themselves. They threaten not just to encrypt information, but to leak sensitive data that they stole to harm victims and their customers or clients—a threat that persists even after the initial ransom is paid. And they have targeted entities that provide critical services and will face disastrous consequences if they do not comply including hospitals and health care providers. Ransomware payments reached over $400 million globally in 2020, and topped $81 million in the first quarter of 2021.[1] The current lack of reliable reporting requirements for enterprises that experience a ransomware attack complicates efforts to measure ransomware's

[1] See https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

true economic impact, but experts agree it runs even higher. The Biden-Harris Administration supports legislative efforts to require cyber incident reporting - including ransomware payments - to both FBI and CISA, that will help prioritize the use of precious resources to support victims, disrupt threat actors and guide future investments to improve resilience.

In short, ransomware attacks leverage systemic weakness in the cyber ecosystem, are costly and pernicious, and undermine confidence in the digital connectivity that underpins our modern economy and offers so much promise for human advancement. Crafting a strategy to stop the scourge of ransomware has been a priority for this Administration.

That strategy begins with an understanding of what makes ransomware so effective. Ransomware takes advantage of key characteristics of the modern cyber ecosystem. First, ransomware actors are able to purchase their tools on the black market and to mount their attacks from leased and disposable cloud-based virtual infrastructure, which they can tear down and rebuild quickly once exposed. Second, the systems these criminals target are too often left vulnerable by failures to patch and upgrade, to properly secure data, to create reliable back-ups, or to ensure frontline employees of targeted organizations consistently exercise basic cybersecurity practices. Third, inconsistent application of anti-money laundering controls to virtual currencies permits criminals to engage in arbitrage and to leverage permissive jurisdictions to launder the proceeds of their crime. Finally, ransomware criminals are too often able to operate with impunity in the nation states where they reside, facing no meaningful accountability for their actions. The Administration's counter-ransomware efforts include action on all these fronts:

Disrupt Ransomware Infrastructure and Actors: The Administration is bringing the full weight of U.S. government capabilities to disrupt ransomware actors, facilitators, networks and to address the abuse of financial infrastructure to launder ransoms.

- The Department of Justice (DOJ) established a task force to enhance coordination and alignment of law enforcement and prosecutorial initiatives combating ransomware. Law enforcement agencies, working through the National Cyber Investigative Joint Task Force (NCIJTF) and with the support of the interagency and foreign partners, are surging investigations, asset recovery, and other efforts to hold ransomware criminals accountable. These efforts bore fruit just last week, when the Department of Justice

announced the arrest of two foreign nationals and the seizure of $6.1 million. Both individuals are alleged to have been members of the REvil ransomware syndicate, which conducted the early July ransomware attack on customers of Kaseya network management software. Two other alleged REvil actors were arrested in Romania, further proof of the success of our international efforts to disrupt the ransomware ecosystem.

- Over the last two months the Department of the Treasury levied its first-ever sanctions against virtual currency exchanges facilitating illicit activity. The exchanges, known as SUEX and Chatex, have been responsible for facilitating ransomware payments to criminals associated with numerous ransomware variants. Treasury will continue to disrupt and hold accountable these ransomware actors and their money laundering networks to reduce the incentive for cybercriminals to continue to conduct these attacks.
- In late September the Department of the Treasury published an updated sanctions advisory encouraging and emphasizing the importance of reporting ransomware incidents and payments to U.S. Government authorities.
- U.S. Cyber Command, the National Security Agency, and the broader Intelligence Community are dedicating people, technology, and expertise to generate insights and options against ransomware actors. Their technical expertise and insights enable and support whole-of-government efforts and operations, including actions against criminals, their infrastructure, and their ability to profit from their crimes.
- The Department of State's Rewards for Justice Office has offered a $10 million reward for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in, or aids or abets, certain malicious cyber activities against U.S. critical infrastructure, to include ransomware activities. Two weeks ago the Department of State also announced an award of up to $10 million for information leading to the identification or location of any individual(s) who hold(s) a key leadership position in the DarkSide ransomware variant transnational organized crime group, which was responsible for the Colonial Pipeline incident, and up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a DarkSide variant ransomware incident.

Bolster Resilience to Withstand Ransomware Attacks: The Administration has called on the private sector to step up its investment in and focus on cyber defenses to meet the threat. The Administration has also outlined the expected cybersecurity thresholds for critical infrastructure and introduced cybersecurity requirements for transportation critical infrastructure.

- The President launched an Industrial Control System Cybersecurity (ICS) Initiative in April—a voluntary, collaborative effort between the federal government and the critical infrastructure community, led by the U.S. Department of Energy in coordination with industry partners. To date, the ICS Initiative has led to over 150 electricity utilities representing almost 90 million residential customers to deploy or commit to deploy control system cybersecurity technologies, bolstering the security and resilience of these facilities. Additional ICS Initiatives have been launched for natural gas pipelines, and will shortly be expanded to the water sector.
- In July, the U.S. Department of Homeland Security (DHS) and DOJ established the StopRansomware.gov website to help private and public organizations access resources to mitigate their ransomware risk.
- The Transportation Security Administration (TSA) at DHS issued two Security Directives, requiring critical pipeline owners and operators to bolster their cyber defenses, enabling DHS to better identify, protect against, and respond to threats to critical companies in the pipeline sector.
- The Office of Intelligence and Analysis at the Department of Homeland Security has prioritized the production of ransomware intelligence at the lowest classification possible and conducts classified and unclassified threat briefings with state, local, and private sector partners across the Nation.
- Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger sent an open letter to CEOs in June communicating best practices to defend against and prepare for ransomware incidents, including backing up data, implementing multi-factor authentication, and testing incident response plans.

- In August, President Biden met with private sector business and education leaders to discuss the whole-of-nation effort needed to address cybersecurity threats—and leaders announced ambitious initiatives to bolster the Nation's cybersecurity.
- The National Institute of Standards and Technology (NIST), within the Department of Commerce, is working with industry to improve current and emerging standards, practices, and technical approaches to address ransomware. Their efforts include the development of the Cybersecurity Framework Profile for Ransomware Risk Management, which builds off the NIST Cybersecurity Framework to provide organizations a guide to prevent, respond to, and recover from ransomware events.
- Treasury and the Department of Homeland Security's CISA are engaging the cyber insurance sector to explore incentives to enhance implementation of cyber hygiene and improve visibility of ransomware activity.

Address the Abuse of Virtual Currency to Launder Ransom Payments: Virtual currency is subject to the same Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls that are applied to fiat currency, and those controls and laws continue to be enforced. The Administration is leveraging existing capabilities, and acquiring innovative new capabilities, to trace and interdict ransomware proceeds.

- The United States remains at the forefront of applying AML/CFT requirements on virtual currency businesses and activities. We continue to hold U.S. virtual currency exchanges accountable to our regulatory requirements, and we have shared indicators and typologies of virtual currency misuse with the virtual currency and broader financial sector through venues like the Financial Crimes Enforcement Network (FinCEN) Exchange program.
- Treasury is leading efforts to drive implementation of international standards on financial transparency related to virtual assets at the Financial Action Task Force and to build bilateral partnerships designed to strengthen AML/CFT controls for virtual currency exchanges overseas. Uneven implementation of international AML/CFT virtual currency standards creates vulnerabilities ransomware actors exploit and inhibits the U.S. Government's ability to disrupt ransomware-associated money laundering.

- Led by the FBI, the Administration is building an Illicit Virtual Asset Notification information sharing partnership and supporting platform to improve the timelines of detecting and disrupting ransomware and other illicit virtual currency payment flows.

Leverage International Cooperation to Disrupt the Ransomware Ecosystem and Address Safe Harbors for Ransomware Criminals: Let me say this plainly: responsible states do not permit criminals to operate with impunity from within their borders. We are working with international partners to disrupt ransomware networks and improve partner capacity for detecting and responding to such activity within their own borders, including imposing consequences and holding accountable those states that allow criminals to operate from within their jurisdictions.

- The Administration is working closely with international partners to address the shared threat of ransomware and galvanize global political will to counter ransomware activities, as reflected in the recent G7 and North Atlantic Treaty Organization joint statements, and Financial Action Task Force efforts, among others. The Administration continues to advocate for expanded membership in, and implementation of, the Budapest Convention and its principles.
- Departments and Agencies continue to engage with foreign nations to improve their capacity for addressing ransomware threats, including through capacity-building that promotes cybersecurity best practices and combats cybercrime, such as trainings on network defense and resilience, cyber hygiene, virtual currency analysis, and other training and technical assistance to foreign law enforcement partners to combat criminal misuse of information technologies.
- The United States remains committed to eliminating safe harbors for ransomware criminals through a more direct diplomatic approach. President Biden has directly engaged President Putin, and established the White House and Kremlin Experts Group to directly discuss and address ransomware activity. The Experts Group continues to meet to address the ransomware threat and to press Russia to act against criminal ransomware activities emanating from its territory. The President has made clear the United States will act to protect our people and critical infrastructure.

To help achieve these and other objectives, I will work in coordination with the Assistant to the President for National Security Affairs and Department and Agency heads, to establish annual cyber priorities and guidance for the Federal government, which will underpin the foundations of our efforts to achieve unity of effort and purposes, and will help Departments and Agencies shape their own planning and operational requirements. Sustaining this unity of effort and unity of purpose will remain a core guiding principle in all that we do. We have the good fortune of having a number of capable agencies at the forefront of securing and defending cyberspace—CISA; the Department of Justice, including the FBI; the Department of Defense; the National Security Agency; elements of the Intelligence Community; the United States Secret Service; the Department of the Treasury; the Department of Energy; and NIST, among others. Their efforts complement one another and strengthen our defense of cyberspace in ways that could not happen in competition or isolation. The Federal government also undertakes a vast array of actions and programs to support and defend the private sector in cyberspace, and ensuring coherence across these lines of effort will be key in ensuring these initiatives are always mutually supporting and never redundant. The more we can support synchronized efforts among Federal agencies, as well as partnerships with the private sector, the greater the return on our investment will be for the American people.

These are daunting undertakings, and overcoming them will require realizing a digital ecosystem that is resilient by design, a policy and commercial environment that aligns actions to consequences, and ensuring public and private sectors are postured to proactively and decisively collaborate. Although ONCD is a young and growing office, we have made significant progress and are building robust relationships with our interagency partners. With the continued confidence and support of this Congress, ONCD will be in a strong position to lead in enhancing the security and resilience of our Nation's cyber ecosystem. Thank you for the opportunity to testify before you today, and I look forward to your questions.