Testimony
of

Iranga Kahangama
Assistant Secretary
Cyber, Infrastructure, Risk and Resilience Policy
Office of Strategy, Policy, and Plans
Department of Homeland Security

Matt Hartman
Deputy Executive Assistant Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Regarding a Hearing on
" ***Combating Ransomware: From Our Small Towns in Michigan to DC"***

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Intelligence & Counterterrorism

June 28, 2022

Introduction

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the Subcommittee, thank you for inviting us to testify today regarding the continued threat of malicious cyber activities, specifically ransomware, and the constant risks posed to Americans, as well as to our businesses and other institutions. Our testimony today highlights the Department of Homeland Security's (DHS) efforts to counter these risks. These efforts are made in coordination with the Biden-Harris Administration's counter ransomware initiatives, and our partners in federal, state, local, tribal, and territorial governments (SLTT), the private sector, and internationally.

Since Under Secretary Silvers and Executive Director Wales testified before your Subcommittee last November, DHS has continued to combat the non-stop threat of cybercrime with several notable successes. However, these cyber threats continue to evolve, and we must therefore continue to evolve the methods that we use to investigate cyber-criminal activity and increase our Nation's resilience against future attacks. Our joint testimony today reinforces that our approach to cybercrime must be multi-pronged. We must pursue a comprehensive strategic approach that prioritizes close partnerships with law enforcement, both domestic and foreign, as well as the private sector, and combines our efforts to:

- disrupt cyber-criminal activity;
- increase resilience of entities and individuals to ransomware incidents;
- target those virtual currency exchanges and online dark marketplaces that enable the ransomware threat through obfuscation of illicit payments;
- investigate transnational cybercrime and organized criminal groups; and
- strengthen foreign law enforcement partner capacity through training and technical assistance.

Most cybercrime is transnational, including ransomware, with criminal activity moving seamlessly across borders. These crimes impact Americans in all 50 states, including Michigan's 8th Congressional district. For example, in 2016, the Lansing Board of Water and Light's administrative services were taken over by hackers as a result of a ransomware attack. Furthermore, in 2020, Michigan State University was a victim of a ransomware attack over Memorial Day. More broadly, DHS does successfully investigate cybercrimes in Michigan. Recently, U.S. Secret Service (Secret Service) agents from the Detroit Field Office successfully investigated a business email compromise case where they were able to return almost $5 million to the victim company.

DHS, in close partnership with the Federal Bureau of Investigation (FBI) and other law enforcement partners, prioritizes investigating cybercrimes, arresting those responsible, and seizing illicit funds and returning them to the victims. In addition, the Department engages the private and public sectors on how to increase their cyber resilience to fend off these attacks.

The Biden-Harris Administration's Approach to Fighting Ransomware

Ransomware threat actors' motives are clear—their goal is profit. These opportunistic criminals go after a wide array of victims—individuals, businesses, hospitals, police departments, and even municipal governments. These criminals encrypt valuable data in an attempt to force their victims to pay ransoms using virtual currencies, with no guarantee the criminal actors will provide a decryption key to restore the victims' files once the ransom is paid. Victims who choose not to pay are saddled with the cost and labor-intensive burden of restoring their systems from backups and, increasingly, threatened with the public release of their stolen data by the criminal actors. The Administration will not allow criminals to hold innocent American citizens and businesses hostage for ransom, or to extort victims with stolen private information, such as health records, without consequence.

The landscape of ransomware actors has undergone several shifts since the Subcommittee's November 2021 hearing, driven in part by the Russian-Ukraine conflict. We observed some ransomware groups adopting political stances, such as the Conti ransomware group's initial pledge of support to Russia at the outset of the invasion of Ukraine. We also witnessed Conti become increasingly emboldened in their demands. For example, in May, Conti threatened to overthrow the Costa Rican government if ransoms were not paid, according to published reports. These criminal actors are resilient and resourceful. When victims stop agreeing to pay ransom, or a ransomware operation is the subject of a law enforcement action, the actors move on to different victims and stand-up new ransomware groups. When victims stop agreeing to pay ransom, or a ransomware operation is the subject of a law enforcement action, the actors move on to different victims and stand-up new ransomware groups.

Therefore, the Department must be equally resilient and resourceful, utilizing a whole-of-government counter-ransomware initiative with domestic and international partners to go after criminals while simultaneously promoting cybersecurity resilience across our critical infrastructure and American businesses. DHS's strategy is multi-pronged: target and dismantle criminal ransomware organizations; target the digital asset ecosystem that criminals use to transfer illicit funds; and increase resilience in our nation's critical infrastructure and public sector, through education and information sharing.

These partnerships continue to pay off in the fight against ransomware as demonstrated in March when an Estonian national was sentenced to 66 months in prison and $36 million in restitution for his role in exploiting stolen financial account information and use of ransomware.[1] The arrest and subsequent indictment were the result of the international partnership between the Secret Service, Latvian State Police, and Estonian Police.

[1] See, "Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes" at, https://www.justice.gov/usao-edva/pr/cybercriminal-connected-multimillion-dollar-ransomware-attacks-sentenced-online-fraud.

Last year Secretary Mayorkas commenced a 60-day sprint as a call for action to tackle ransomware.[2] As a result, DHS, along with colleagues across the U.S. Government, launched "StopRansomware.gov,"[3] our official central website for resources from across the Federal Government community to tackle ransomware more effectively. The purpose of this website is to help public and private organizations defend against the rise in ransomware attacks by providing guidance on protection, detection, and response all on a single website. As of June 2022, StopRansomware.gov received over 280,000 visits.

The Cybersecurity and Infrastructure Security Agency Efforts on Ransomware

One of the Cybersecurity and Infrastructure Security Agency's (CISA) core functions is to foster resilience. It played a leading role for DHS in launching "StopRansomware.gov." In January 2021, CISA launched a "Reduce the Risk of Ransomware" awareness campaign.[4] This campaign promoted resources and best practices to mitigate the risk of ransomware and focused on supporting COVID-19 response organizations and K-12 institutions. Further, CISA expanded its publicly available information to include a ransomware guide, fact sheets, toolkits, online training resources, and educational webinars.

CISA continues to take many proactive steps to prevent ransomware . These efforts include hundreds of engagements focused on cybersecurity and combatting ransomware. CISA routinely engages with SLTT partners, including events specifically for governors and county leaders, as well as the private sector. In addition, CISA continues to release cyber alerts containing technical details and mitigation measures. These alerts, often issued jointly with interagency partners and increasingly with foreign partners, provide timely information about current security issues, vulnerabilities, and exploits. Several recent examples include information on BlackMatter ransomware, Conti ransomware, and ongoing cyber threats to water and wastewater systems. Effective confrontation of the ransomware threat relies on visibility and awareness, which CISA provides through email and other subscription services.

Visibility and awareness also require information sharing and collaboration. In August 2021, CISA launched the Joint Cyber Defense Collaborative (JCDC) to lead the proactive development of the Nation's cyber defense plans, which outline activities to reduce the prevalence and the impact of cyber intrusions, such as ransomware. JCDC promotes national resilience by coordinating actions to identify, protect against, detect, and respond to the

---

[2] *See Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience* (March 31, 2021), available at https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience.
[3] *See New StopRansomware.gov Website – The U.S. Government's One-Stop Location to Stop Ransomware* (July 15, 2021), available at https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location.
[4] *See CISA Launches Campaign to Reduce the Risk of Ransomware* (Feb. 16, 2021), available at https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware.

malicious cyber activity targeting U.S. critical infrastructure or national interests. Building on the authorities included in the Fiscal Year (FY) 2021 National Defense Authorization Act, the JCDC includes the joint cyber planning office, but recognizes that that there is a full suite of capabilities necessary to truly make a difference for our Nation's cybersecurity posture. The JCDC brings together leading technology, communications, and incident response companies, as well as all relevant federal agencies, to unify and integrate prevention and response planning. The JCDC establishes a unique entity that can *proactively* provide visibility into a common operating picture of the threat environment through close partnership with the private sector and the federal cyber ecosystem.

The Nation's security and resilience in the face of the ransomware threat relies on a collective, unified approach across the federal government that combines the full suite of relevant interagency authorities and capabilities. As designated in the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA), CISA will establish a Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks. CISA and the FBI will serve as co-chairs of this federal task force, which will organize and orchestrate the spectrum of U.S. Government activities to address the ransomware threat, from protection and mitigation to intelligence prioritization and disruption.

DHS Investigative Efforts to Combat Cybercrime

The world's economy is rapidly changing and becoming more digitized. In partnership with international law enforcement partners, the Secret Service has achieved notable successes in combatting cyber-enabled financial crimes, including dismantling two early centralized virtual currency providers that supported extensive criminal activity: e-Gold Ltd.[5] and Liberty Reserve.[6] Additionally, in 2020, the Secret Service, with domestic and international partners, successfully investigated a Russia-based criminal scheme.[7] The investigation led to the seizure of millions in cryptocurrency and indictments of two Russian nationals.

Central to these successes is the global network of 44 Secret Service-led Cyber Fraud Task Forces (CFTFs). The mission of these CFTFs is to partner with SLTT and foreign law enforcement agencies, private and public sectors, and academia for information sharing and conducting joint investigations. The Secret Service also operates 19 international attaché offices

[5] *See*, U.S. Department of Justice: "Over $56.6 Million Forfeited In E-Gold Accounts Involved In Criminal Offenses," https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses; Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

[6] *See*, U.S. Department of Justice press releases: "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business," https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital; "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme," https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

[7] *See*, "Russian Nationals Indicted for Conspiracy to Defraud Multiple Cryptocurrency Exchanges and Their Customers," https://www.justice.gov/usao-ndca/pr/russian-nationals-indicted-conspiracy-defraud-multiple-cryptocurrency-exchanges-and; "Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft," https://home.treasury.gov/news/press-releases/sm1123.

around the world, partnering with the global law enforcement community to combat transnational financial crimes.

Participation in these task forces is bolstered through Secret Service-led law enforcement training programs at the National Computer Forensics Institute (NCFI). At NCFI, the Secret Service trains SLTT law enforcement personnel, prosecutors, and judges on preventing, mitigating, and responding to malicious cyber activities, including ransomware. Personnel who receive training serve as force multipliers complementing Secret Service CFTFs. Currently the NCFI's authorizing legislation (6 U.S.C. § 383) limits NCFI to training SLTT law enforcement officers. Congress is currently considering legislation to re-authorize NCFI, which could incorporate an authorization to train foreign partners.[8] In addition, Homeland Security Investigations (HSI) and Secret Service agents regularly participate in capacity building workshops delivered through the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN), a U.S. State Department Bureau for International Narcotics and Law Enforcement Affairs (INL)-funded initiative where digital forensics experts and long-term federal agents deliver training and technical assistance to foreign partners that enables them to better cooperate with U.S. authorities, including on ransomware and criminal misuse of cryptocurrency investigations.

Today, the Secret Service coordinates, integrates, and shares information on ransomware cases through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), where a Secret Service agent leads the Criminal Mission Center. Through the NCIJTF, the Secret Service works hand in hand with partners from the Departments of Justice, including the FBI, State, Treasury, and other domestic and foreign partners. The Illicit Virtual Asset Information Notification system, a joint effort between multiple agencies, operates from the NCIJTF and, once fully operational, will enable increased partnership between federal law enforcement and the private sector to detect and disrupt ransomware and other illicit virtual currency payment flows.

U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has 80 offices in over 50 countries and works to combat cybercrime, including ransomware, through its Cyber Financial Section of the Financial Crimes Unit, which provides training to international partners and analytical assistance in tracing digital assets. In addition, HSI's Cyber Crimes Center (C3) has led numerous cyber-related trainings with foreign law enforcement partners. In 2020, HSI, working with the Departments of Justice and the Treasury, dismantled three terrorist financing cyber-enabled campaigns – involving al-Qaeda, Hamas's al-Qassam Brigades, and ISIS.[9] Since January 2020, HSI C3 conducted in-person and virtual training covering online investigations, dark web, and cryptocurrency investigations for law enforcement partners in over 20 countries. Some of this training was conducted in coordination

[8] H.R.7174 - National Computer Forensics Institute Reauthorization Act of 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/7174

[9] *See*, "Global disruption of 3 terror finance cyber-enabled campaigns," Global disruption of 3 terror finance cyber-enabled campaigns | ICE.

with the HSI Financial Crimes Unit. For example, in May 2022, HSI C3 provided network intrusion investigations training to law enforcement officials in Panama.

Additionally, HSI initiated Operation Cyber Centurion, a cyber threat intelligence initiative that proactively detects vulnerabilities in critical infrastructure and works with victims to remediate the vulnerabilities before they are exploited. These vulnerabilities are often used to enable the theft of sensitive data or the disruption of a functioning system and are commonly used in ransomware attacks. Cyber Centurion is designed to significantly disrupt adversary plans to exploit the internet to subvert U.S. laws and threaten the economic integrity, public safety, and national security of the United States. The initiative is in alignment with CISA's priorities for the protection of critical infrastructure.

DHS is committed to strengthening the law enforcement capabilities of Secret Service, HSI, and other law enforcement partners to investigate all forms of cybercrime within our authorities and arrest those responsible.

International Partnerships

Cyber-criminals and nation-state actors will continue to view ransomware as an effective means to fund themselves and cause disruptive effects in critical infrastructure. It will take a global effort to stop them. To combat transnational cybercrime, including ransomware, both the Secret Service and HSI maintain close partnerships with a wide array of foreign law enforcement agencies. The Secret Service is the first U.S. law enforcement agency to have permanent representation at Europol with an attaché assigned to the Joint Cybercrime Action Taskforce at Europol's European Cyber Crime Centre.

In March, DHS hosted the Cross-Border Crime Forum with our Canadian partners to make our nations safer and committed to working together to combat ransomware, strengthen security and resilience of critical infrastructure against these threats, as well as increase reporting of ransomware incidents. In May, DHS leadership attended the Ottawa 5 meeting in London, where discussions focused on combatting ransomware.

Last fall, the United States hosted a Counter-Ransomware Initiative meeting with international partners from more than 30 countries. Delegates discussed common challenges, approaches, and opportunities to advance international cooperation to achieve shared goals. DHS serves as the lead for the U.S. on the sub-group focused on resilience. DHS, together with the Departments of Justice, State, and Treasury, also recently participated in the initial meeting of the U.S.-EU Ransomware Working Group.

The Department continues to work together with like-minded foreign partners to target, identify, and prosecute cybercriminals, disrupt their malicious IT infrastructure, and shut down financial networks used to launder illicit proceeds. In April 2022, the Secret Service announced that an international operation, organized by Europol and conducted in partnership with the FBI,

resulted in the seizure of the RaidForums website—a popular marketplace for cybercriminals to purchase and sell hacked data. This successful outcome was the result of combined efforts between the Secret Service, other Federal agencies, as well as international partners, including the United Kingdom's National Crime Agency.[10]

Conclusion

The Department commends Congress for passing the FY22 Omnibus Appropriations bill, which passed in March and included the language from CIRCIA. In addition, we greatly appreciate Congress' continued support for the cyber training of SLLT law enforcement. Centers such as the NCFI provide critical cyber investigation skills and tools to our partners needed to prevent, mitigate, and respond to cyber incidents.

DHS is committed to countering the cybercrimes targeting our country, our citizens, and our partners around the world. We are grateful for the continued support of Congress and to our fellow departments and agencies for their support in this effort. Together we can ensure the success of DHS' multipronged mission to increase cyber resilience, disrupt the ransomware ecosystem, and hold accountable those who commit these crimes. Thank you again for the opportunity to testify and we look forward to your questions.

[10] *See*, "U.S. Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator," https://www.justice.gov/usao-edva/pr/us-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator