Testimony
of

Robert Silvers
Under Secretary
Office of Strategy, Policy, and Plans
Department of Homeland Security

Brandon Wales
Executive Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Jeremy Sheridan
Assistant Director of Investigations
U.S. Secret Service
Department of Homeland Security

Regarding a Hearing on
"***A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role"***

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation
and Subcommittee on Intelligence & Counterterrorism

November 17, 2021

Chairwoman Clarke, Chairwoman Slotkin, Ranking Member Garbarino, Ranking Member Pfluger, and distinguished members of the Subcommittees on Cybersecurity, Infrastructure Protection, & Innovation and on Intelligence and Counterterrorism, thank you for inviting us to testify regarding the continued threat of ransomware and the constant risks it poses to the American people. Our testimony today highlights the Department of Homeland Security's (DHS) efforts to counter these risks. These efforts are made in coordination with the Administration's counter ransomware initiatives, and our partners in federal, state, local, tribal, and territorial governments, the private sector, and internationally.

Our joint testimony today reinforces that we cannot approach the problem of ransomware by looking at only one aspect of the threat. We must tackle ransomware through a comprehensive strategy that includes close partnerships with the private sector and integrates the collective efforts to:

- disrupt cyber criminals;
- build resilience of entities and individuals;
- improve oversight of and, where appropriate, enforcement against virtual currency exchanges and online dark marketplaces that enable the ransomware threat;
- apply diplomatic pressure on countries that harbor ransomware perpetrators; and
- forge coalitions of like-minded countries to collectively counter the threat.

All of these efforts involve international cooperation to eliminate the safe havens and opportunities for ransomware actors. Please allow us to discuss some of the efforts underway at DHS, across the U.S. Government, and with our domestic and foreign partners to combat ransomware.

The Administration's Approach to Ransomware

Ransomware is a financially motivated crime. Ransomware attackers extort vulnerable organizations and individuals. They obligate their victims to pay ransoms using virtual currencies in order to regain access to critical data, restore IT functions, and prevent the stolen data from being disclosed. But the cost to society is more than the ransom. We have seen too frequently the operational disruptions and downstream national impacts that can result from ransomware. We have seen hospitals, municipal governments, schools, police departments, and other essential businesses and organizations taken offline. Earlier this year we experienced a disruption to our gasoline supply resulting from a ransomware attack against Colonial Pipeline. And we saw certain food prices rise following an attack on a major meat processor, JBS. We recognize the stakes and are all-in to address this scourge.

The Administration is spearheading a whole-of-government counter-ransomware initiative that is working with partner nations to disrupt and deter ransomware actors while simultaneously promoting resilience and cybersecurity across our critical infrastructure and private businesses. Through this initiative, we are targeting criminal actors for apprehension and prosecution. We are targeting and dismantling the infrastructure used to conduct these attacks.

We are targeting the illicit financial gains these actors seek, as well as the unlawful financial networks used to move, launder, and conceal illicit profits. We are increasing resilience in our critical infrastructure, and the private and public sectors in general, through cyber education and awareness and sharing information on tactics used by our adversaries. One example of these efforts is the U.S. Treasury Department's recent announcement of sanctions on the Russia-based SUEX cryptocurrency exchange for facilitating transactions involving illicit proceeds from at least eight ransomware variants. This was the first time such actions were taken against a cryptocurrency exchange. We will continue to do more to effectively disrupt this threat.

The Department of Homeland Security's Sprint to Combat Ransomware

We are here today to talk about the significant efforts DHS is making to support the Administration's counter-ransomware initiative. In February 2021, Secretary Mayorkas issued a call for action to tackle ransomware more effectively. In March, DHS launched a 60-day sprint to combat ransomware.[1] This was the first of six cyber-focused sprints and was intended to elevate existing efforts and remove roadblocks hampering progress. Through the Secretary's leadership and leveraging the unique capabilities of DHS Components, we took action to increase resilience, and disrupt criminal use and development of ransomware.

During this sprint, Secretary Mayorkas and Attorney General Garland participated in the annual Five Country Ministerial, which issued a "Ministerial Statement Regarding the Threat of Ransomware."[2] Many Components within DHS played an active role. The U.S. Secret Service held a virtual cyber incident response simulation with state and local governments focused on ransomware, and the Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the U.S. Treasury Department, engaged with the cyber insurance industry on ransomware. The U.S. Coast Guard held exercises to synchronize Coast Guard and state incident response, and numerous U.S. Immigration and Customs Enforcement (ICE) symposia, panels, and discussions were held on cybercrime and ransomware.

As a natural progression of the sprint, in July DHS led, along with colleagues across the U.S. Government, the launch of "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.

---

[1] *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.
[2] *See Five Country Ministerial Communiqué* (April 9, 2021), available at https://www.homeaffairs.gov.au/news-media/archive/article?itemId=596.
[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.

The Department's sprint efforts are ongoing. Through multiple DHS agencies, we continue to work with our state, local, tribal, and territorial partners to build awareness, promote preparedness, and improve resilience. We continue to work with these same partners to build investigative capability through programs like the National Computer Forensic Institute (NCFI). We continue to promote preparedness and resilience across critical infrastructure and across the private sector.

The Cybersecurity and Infrastructure Security Agency Efforts on Ransomware

One of CISA's core functions is to foster such 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 has also taken many proactive steps to prevent the ransomware threat. These efforts include hundreds of engagements focused on cybersecurity and combatting ransomware. CISA routinely engages with state, local, tribal, and territorial partners, including events specifically for governors and county leaders; and for 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, 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, and CISA provides that through email and other subscription services.

Visibility and awareness also require information sharing and collaboration. CISA launched the Joint Cyber Defense Collaborative (JCDC) to lead the 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 malicious cyber activity targeting U.S. critical infrastructure or national interests. Building on the authorities included in the Fiscal Year 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 will bring 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 is uniquely the only federal cyber entity that *proactively* provides visibility into the common operating picture of the threat environment through partnership with the private sector and the federal cyber ecosystem.

---

[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.

The U.S. Secret Service Efforts on Ransomware

For more than 150 years, the U.S. Secret Service has investigated financial crimes. Following the proceeds from ransomware attacks is no different. With the support of its partners, the Secret Service has shut down a number of illicit cryptocurrency exchangers that facilitated the laundering of criminal proceeds, including proceeds from ransomware. The Secret Service's successes include working with partners to shut down Western Express in 2013 and BTC-e in 2017,[5] both of which served as key laundering platforms for cyber criminals.

Secret Service Cyber Fraud Task Forces (CFTFs), located domestically and internationally, are at the forefront of investigating cyber-enabled financial crimes. CFTFs partner with state, local, tribal, and territorial (SLTT) law enforcement, private and public sectors, to include financial institutions, and academia. An additional significant effort is made through the NCFI. This federally-funded facility provides training courses to SLTT law enforcement, prosecutors, and judges at no cost to the attendees or their agencies. Attendees, who receive training on cyber response and investigation, to include ransomware, act as force multipliers for Secret Service CFTFs. Operation Zydeco in 2019[6] is one such example, where SLTT members of the Secret Service Louisiana CFTF trained by NCFI responded to a ransomware attack targeting a sheriff's office. In October 2021, NCFI hosted a virtual cyber incident response competition to test the technical skills of SLTT law enforcement as a federal/state group responding to a ransomware incident.

Today, the U.S. Secret Service coordinates, integrates, and shares information on its ransomware cases through the 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, State, the Treasury, and other domestic and foreign partners. This collaborative approach to investigating cybercrime is essential in pooling government resources and skillsets to best combat ransomware actors and their networks. The Secret Service also continues to reinforce its international partnerships.

Ransomware actors are geographically dispersed; disrupting them requires the cooperation of international law enforcement agencies to locate, arrest, and hold these actors accountable for criminal activity. The Secret Service fosters collaboration, developed and built upon years of cooperation, through direct partnership with foreign law enforcement agencies and international law enforcement organizations like INTERPOL and Europol. An example of this was the February agreement of a Canadian-American citizen, Ghaleb Alaumary, to plead guilty

---

[5] *See Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox* (July 26, 2017), available at www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

[6] *See Louisiana Sheriff's Office Targeted in Cyberattack Attempt* (Dec. 16, 2019), available at https://apnews.com/article/c2c78e08b8e82791ada335ce9f8dbf5f.

to two counts of conspiracy to commit money laundering, including laundering funds from a 2019 North Korean-perpetrated cyber-heist of a Maltese bank.[7] In September, Alaumary was sentenced to more than 11 years in federal prison and was required to pay more than $30 million in restitution to victims.[8] This case highlights the transnational nature of criminal organizations engaged in these sorts of crimes.

Efforts by the Secret Service, ICE, and other law enforcement partners to hold criminal actors responsible are ongoing, as well as efforts to strengthen law enforcement capabilities to counter the threat of ransomware.

International Efforts

The United States cannot combat this threat alone. We must continue to work alongside our international partners, strengthening existing relationships, and forging new ones. Together we must stand united to support the adoption of, and adhere to, international cyber norms and condemn countries who violate these norms or harbor cyber criminals, or support their criminal activities.

In late October, the United States hosted a Counter-Ransomware Initiative meeting with like-minded international partners from more than 30 countries. Delegates had an open discussion on common challenges, approaches, and opportunities to advance international cooperation to achieve shared goals. DHS, together with the Departments of Justice, State, and the Treasury, also recently participated in the initial meeting of the U.S.-EU Ransomware Working Group. This effort is the result of an agreement between the Secretary of Homeland Security and Commissioner Johannsen of the European Commission to explore joint solutions to this global problem. The Department also participates in a ransomware working group with the Republic of Korea and through the Five Country Ministerial. These meetings and the scope of participation confirm ransomware is not just an issue for the United States.

The Department continues to work together with like-minded international partners to target, identify, and prosecute cyber criminals, disrupt their IT infrastructures, and shut down financial networks used to launder illicit proceeds. We collaborate and share active threat intelligence and cybersecurity best practices to reinforce international societal norms for responsible behavior in cyberspace and call out countries who choose not to follow these norms and instead harbor criminal cyber actors or facilitate criminal behavior.

---

[7] *See Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe* (Feb. 17, 2021), available at https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[8] *See International Money Launderer Sentenced to More Than 11 Years in Prison for Laundering Millions of Dollars in Cyber Crime Schemes* (Sept. 8, 2021), available at https://www.justice.gov/opa/pr/international-money-launderer-sentenced-more-11-years-prison-laundering-millions-dollars.

Legislative Initiatives to Assist on Ransomware

We commend Congress for passing the *Infrastructure Investment and Jobs Act*, which includes funding to increase cyber resilience for critical infrastructure that will help prevent ransomware attacks. We also acknowledge and applaud some of the ongoing efforts in Congress that would significantly help in the fight against ransomware.

*Cyber Incident Reporting Legislation***:** Our ability as a Department to bolster resilience and investigate criminal actors depends on us learning about ransomware attacks and other malicious cyber activity. As such, we support legislation requiring the reporting of cyber incidents. This information is critical for understanding national risk and taking actions to disrupt and deter additional malicious activity. We cannot accurately address a problem if we do not understand its scale and scope. Cyber incidents are underreported. Additional legislative steps and new authorities are necessary to understanding the full scope of the ransomware problem.

Support for the Training of State, Local, Tribal and Territorial Law Enforcement: We appreciate Congress' continued support for the cyber training of SLLT law enforcement. Centers such as the NCFI provide critical cyber investigation skills to our partners who are often the first responders to ransomware attacks and act as force multipliers.

*Law Enforcement Capabilities to Counter Cyber Crime***:** The U.S. Secret Service and ICE's Homeland Security Investigations have robust capabilities to investigate criminal cyber activity, including ransomware attacks. Expanding these capabilities to include investigating money laundering associated with digital assets would give the Department an additional tool to prevent cyber criminals from profiting from their illicit gains.

These legislative actions would increase our ability to address the threat posed by ransomware.

Conclusion

DHS is committed to countering the threat of ransomware facing our country, our citizens, and our allies around the globe. 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 increase cyber resilience and disrupt and hold accountable those who perpetrate these acts. Thank you again for the opportunity to testify today and we look forward to your questions.