THE WHITE HOUSE
WASHINGTON

FOR IMMEDIATE RELEASE
November 1, 2023

FACT SHEET: Biden-Harris Administration Convenes Third Global Gathering to Counter Ransomware

The Biden-Harris Administration remains committed to taking bold actions to combat ransomware. Ransomware is a global scourge requiring international cooperation to disrupt. This week, the White House convened International Counter Ransomware Initiative (CRI) for its third meeting in Washington, D.C., bringing together 50 members, including 48 countries and representatives from the European Union and INTERPOL, to discuss new operational projects and develop concrete policy commitments.

This year, the initiative welcomed thirteen new members—Albania, Colombia, Costa Rica, Egypt, Greece, INTERPOL, Jordan, Papua New Guinea, Portugal, Rwanda, Sierra Leone, Slovakia, and Uruguay—who participated in the gathering along with Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, the Czech Republic, the Dominican Republic, Estonia, the European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Poland, the Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, Ukraine, the United Arab Emirates, the United Kingdom, and the United States.

At the gathering, CRI members advanced the Initiative's commitments to resilience, cooperation, and disruption through the CRI's Policy Pillar, Diplomacy and Capacity Building Pillar, and the International Counter Ransomware Task Force (ICRTF). The

Policy Pillar spearheaded efforts to undercut the business model that underpins the ransomware ecosystem by building the CRI's resources on cyber insurance, victim behavior, seizure and confiscation of virtual assets, ransom payments, and best practices for incident reporting and information sharing. The Diplomacy and Capacity Building Pillar expanded the CRI's partnerships with the addition of thirteen new members to the coalition. The ICRTF launched information sharing across all 50 members of the CRI by disseminating operational tools.

This year's convening of the CRI focused on **launching capabilities to disrupt attackers and the infrastructure they use to conduct their attacks, improving cybersecurity through sharing information;** and **fighting back** against ransomware actors. Together, members of the CRI took bold new action to further advance the initiative, including:

- **Launching Capabilities:** Leading a **mentorship and tactical training program** for new CRI members to build their cyber capacity. The initiative will also launch a project to **leverage artificial intelligence** to counter ransomware.

- **Information Sharing:** The CRI launched innovative information sharing platforms enabling CRI member countries to rapidly share threat indicators, including Lithuania's Malware Information Sharing Platform (MISP) and Israel and the UAE's Crystal Ball platform. Additionally, a CRI website will be built and maintained by Australia, which will include a forum for members to request assistance from CRI members.

- **Fighting Back Against Bad Actors:** CRI members endorsed the first-ever joint CRI policy statement declaring that member governments should not pay ransoms. The initiative will also create a shared blacklist of wallets through the U.S. Department of the Treasury's pledge to share data on illicit wallets used by ransomware actors with all CRI members. Members have also committed to **assist any CRI member with incident response** if their government or lifeline sectors are hit with a ransomware attack.

The International Counter Ransomware Initiative celebrated notable successes since its last convening, including: increased capacity amongst members; improved cybersecurity through sharing information; enhanced capabilities to block attackers and the infrastructure they use to conduct their attacks; arrests of ransomware actors and financial disruptions. More notable success are addressed below.

The CRI Policy Pillar

Over the course of 2023, Singapore and the United Kingdom drove discussions on levers to address key policy questions in the fight against ransomware. Singapore, supported by the Financial Action Task Force (FATF) authors of FATF's Counter Ransomware Financing report and the Institute of Security and Technology (IST), led an intersessional meeting to improve members' understanding of the ransomware payments ecosystem. In addition, by encouraging CRI members to implement FATF Recommendation 15 on Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) for Virtual Asset Service Providers, the Policy Pillar forged sharper interventions to disrupt the illicit financial flows that fuel the ransomware industry.

The United Kingdom led a research project examining how **victims** behave during an attack, aiding the CRI's understanding of what circumstances lead victims to pay ransoms, whether they report the payment, and what effects both of these behaviors have on the victim and offender. The Netherlands led research on crypto and **virtual asset seizures**, recommending best practices and tools that the CRI countries can use to engage providers. France led research on the **cyber insurance landscape** to identify areas for policy intervention**,** and Singapore led the development of best practices on cyber **incident reporting and information sharing.**

Through the Policy Pillar, CRI members affirmed the importance of adopting strong and aligned messaging discouraging paying ransomware demands and leading by example. CRI members **endorsed a statement that relevant institutions under our national government authority should not pay ransomware extortion demands.** This shows unity and consensus with setting a new global norm and standard

around ransomware payments.

The CRI provides an opportunity to further reshape the cyber environment by creating long-term cooperative approaches and common understandings of **accountability in cyberspace**, consistent with international law as well as state actions as embodied in the Framework for Responsible State Behavior in Cyberspace, endorsed by all United Nations member states.

Over the next year, the CRI Policy Pillar will continue to build international cohesion and collaboration on counter-ransomware policies by expanding the work done in 2023. Possible projects include, but are not limited to, formalizing CRI processes, by determining potential governance frameworks for CRI members, exploring how partnerships with the cyber insurance industry can help in countering ransomware, and how countries should work together to raise the overall cybersecurity posture against ransomware attacks through cybersecurity standards and best practices, including in areas such as artificial intelligence and other emerging technologies.

The CRI Diplomacy and Capacity Building Pillar

The Diplomacy and Capacity Building Pillar expanded the CRI's reach by adding **thirteen new members** to the coalition and incorporating capacity building efforts throughout all the CRI's efforts. Major efforts included developing guidelines for joining the Initiative, establishing an onboarding and mentorship process for new members, and finding opportunities to promote the CRI to potential new members. For example, this summer some CRI members convened at the George C. Marshall European Center for Security Studies in Germany to support a CRI component to a cyber capacity building initiative for African nations.

Over the next year, the Pillar will continue to recruit new members and will develop a robust capacity building program for new members that includes designing tailored capacity building workshops in response to members' needs.

The International Counter Ransomware Task Force (ICRTF)

The ICRTF—established at last year's convening and led by Australia this year—built **operational projects and platforms** informed by the findings and outcomes presented at the 2022 CRI gathering. The CRI website, maintained by Australia, will include a **forum for members to request assistance** from CRI members to respond to specific ransomware incidents to ensure offers of support are streamlined and well-coordinated. The ICRTF will also continue to support transnational operations and leverage existing **law enforcement collaboration platforms**.

Israel and the UAE announced access for CRI members to their joint information sharing project **Crystal Ball**, enabling CRI members to access tools such as databases, virtual coordination platforms and contact lists. Lithuania built the CRI **Malware Information Sharing Project** (MISP) instance, an open-source solution for sharing threat intelligence. India unveiled the **Trident Resilience Platform**, which offers malware analysis, remediation, and awareness functions. Italy launched a pilot for ICRTF members of the **Cybersecurity Authorities Network** (CyAN), a platform for building a common knowledge base at the political, strategic, and operational levels of counter-ransomware efforts.

All four projects—Crystal Ball, MISP, Trident, and CyAN— will soon be interoperable, opening channels of communication, analysis, and transparency across the like-minded partnership of the CRI and contributing actionable information to the initiative.

The **Netherlands** delivered a **Ransomware Targeting Framework** to enable CRI members to prioritize criminal targets and the services which support the ransomware ecosystem. **Poland** led the **RACER project**, an operational set of recommendations for governments to use for the prevention, reporting, and post-incident evidence-gathering and forensics of ransomware incidents. The **United States** and **Spain** worked with the Institute for Security and Technology (IST) to develop **case studies** on how public-private partnerships can best be leveraged to fight ransomware.

Building on the information sharing established in its inaugural year, the ICRTF will hold regular **virtual seminars** on ransomware-related topics in 2024. A **comparative**

analysis of national and regional threat assessments will build a global, comprehensive landscape of the ransomware threat picture for the CRI. Additionally, the ICRTF will create, compile, and share resources to develop its members' national capabilities. This commitment includes developing a **guide to create a national counter ransomware task force**. The Task Force will also continue to produce periodic reports for CRI members.

The work of the CRI is making a difference for our countries and our communities in their schools, hospitals, and homes. Over the next year, the coalition plans to provide rapid assistance to CRI members if their government or critical sectors are hit with a ransomware attack, continue to share actionable information with CRI partners, and enhance cyber capacity building through mentorship of new members and tactical training through ICRTF.

###