STATEMENT FOR THE RECORD

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEES ON BORDER SECURITY AND ENFORCEMENT AND CYBERSECURITY AND INFRASTRUCTURE PROTECTION

"Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans"

Tuesday, April 21, 2026 | 10:00 a.m.

TESTIMONY OF

CYNTHIA KAISER

Senior Vice President, Halcyon Ransomware Research Center

Former Deputy Assistant Director, FBI Cyber Division

I. Introduction

Chairman, Ranking Member, and distinguished Members of the Subcommittees: thank you for the opportunity to appear before you today. My name is Cynthia Kaiser. I currently serve as Senior Vice President of the Halcyon Ransomware Research Center, where my team tracks, analyzes, and publishes research on ransomware actors and their impact on American society. Before joining Halcyon, I spent two decades at the Federal Bureau of Investigation, most recently as Deputy Assistant Director of the FBI Cyber Division. I have dedicated my career to understanding and dismantling the criminal networks that target our citizens, our institutions, and our way of life.

I appear today representing Halcyon, a cybersecurity company whose mission is to defeat ransomware—the most disruptive and dangerous form of cybercrime afflicting America today. I commend this Committee for convening this hearing. The President's recent Executive Order 14390 on Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens correctly identifies these threats as top-tier national security concerns and calls for a whole-of-government response. I am here to reinforce that call, ground it in data, and offer concrete ideas for what more we can and must do.

I want to begin with a statement that I believe this Committee, and every American, should hold in mind throughout this hearing: the people perpetrating these crimes are not merely technical actors engaged in financial misconduct. They are predators. They are callous. They are, in many cases, knowingly endangering and ending human lives—and they do not care. This Committee has the power to ensure that they face serious consequences for the harm they chose. For the harm they have caused.

II. The Scale and Human Cost of Cybercrime Against Americans

The FBI's Internet Crime Complaint Center released its 2025 Internet Crime Report earlier this year. The picture it paints should make every American angry—and I mean genuinely, viscerally angry. Let me walk you through why.

In 2025 alone, cybercriminals stole over $20 billion from Americans. That is not a Pentagon budget line or an abstract economic figure—it is a generation worth of wealth: retirement savings wiped out, small businesses destroyed, families left without resources they spent a lifetime building. Over 75,000 Americans were victimized by sextortion schemes last year. During a single FBI operation described in that report, 38 victims were referred to an FBI Victim Specialist for suicide intervention. Thirty-eight people so devastated by cybercrime that agents feared victims would take their own lives.

Ransomware is growing in size and in ability. We know that reports to FBI only represent a fraction of attacks and crime against US organizations and citizens. Even so, ransomware attacks reported to the FBI have increased by over 20 percent since 2023.

Attacks that used to take weeks, now take just a few hours. AI has made it a lot easier for our adversaries to lie, and they are tricking more and more people into giving them access to company networks. Thousands of US businesses are attacked every year, and private sector data indicates that ransomware gangs target small and medium-sized businesses four times as often as large organizations.

The even sharper increase that FBI reported in ransomware attacks against critical infrastructure is especially worrisome. Last year, healthcare overtook all other critical sectors to become the single most targeted industry for ransomware. Attacks against hospitals and medical facilities nearly doubled, from 238 attacks in 2024 to 460 in 2025. Attacks against critical manufacturing and financial services also hit record highs, each increasing by close to 40 percent. Criminal organizations focused on these sectors because of deliberate strategic choices they made to maximize harm and maximize payment.

I want the Members of this Committee to sit with that healthcare number for a moment: 460 ransomware attacks on American hospitals and health systems in a single year. That is more than one attack every single day, targeting the places Americans go when they are most vulnerable—when they are giving birth, receiving cancer treatment, or fighting for their lives in an emergency room.

A. These Adversaries Are Making Deliberate Choices to Target the Vulnerable

When ransomware gangs shifted their targeting to hospitals, it was not an accident. It was a business decision. Ransomware actors—who are criminal entrepreneurs as much as they are hackers—have calculated that hospitals, facing life-or-death consequences for every minute of downtime, are more likely to pay ransoms than other targets. They are explicitly leveraging the fragility of human health to maximize their profits.

Healthcare was once considered an informal off-limits target even within criminal ransomware communities. That is no longer the case. These actors have looked at children in NICUs, at dialysis patients, at trauma centers serving rural communities where the next nearest hospital is 70 miles away—and they have decided those patients are acceptable collateral damage, even useful leverage. That is more than just recklessness. It is a moral choice. And I think we can all agree: it is one of the most reprehensible moral choices a person can make.

Research published by the University of Minnesota, linking a database of hospital ransomware attacks to Medicare claims data, found that ransomware attacks on hospitals caused at least 47 deaths between 2016 and 2021. That number is certainly higher today. When a hospital is taken offline, ambulances are diverted. Labs are shuttered. Surgeries are postponed. For a heart attack or stroke patient, the difference of even one hour in receiving treatment can mean death or permanent disability. The hackers responsible for these attacks know this. They are not naïve. They have simply decided that these deaths are someone else's problem.

If a contractor knowingly tampered with the medical equipment of critically ill patients to extort money from a hospital, we would not debate what degree of crime had been committed. We would prosecute them to fullest extent of the law. Perpetuating this type of attack on a computer does not change the crime, and it should not change the punishment.

III. Ransomware is Organized, Professional, and Without Moral Constraint

I want to address something that I believe is sometimes lost in the technical and policy discussion about cybercrime: the character of the people doing these acts.

The most active ransomware groups—Akira, Qilin, INC, Play, and others identified in the FBI's 2025 report—operate like businesses. They have HR processes. They have branding. Some have customer service lines for victims trying to negotiate ransom payments. They are organized, professional, and utterly without moral constraint when it comes to the harm they cause.

Our grandparents, our small businesses on Main Streets, our doctors—none of them should live in fear about what someone might be doing on a keyboard thousands of miles away.

But the current legal and policy response does not consistently reflect that reality. The FBI and its partners are doing extraordinary work with the authorities they have. But the gap between the severity of these crimes and the consequences that follow needs to close.

The Halcyon Ransomware Research Center identified 70 new ransomware variants last year alone—on top of 67 identified by FBI the year before. Criminal ransomware ecosystems are adaptive, decentralized, and self-replenishing. Two of last year's new groups, Lynx and Dragonforce, rose within months to become among the highest-volume ransomware operators worldwide. When law enforcement dismantles one group, others fill the void unless we are also raising the cost and risk of entry into this business. We are not doing that sufficiently today.

IV. The President's Executive Order and National Cyber Strategy: A Strong Foundation

Executive Order 14390, signed March 6, 2026, reflects a welcome and necessary escalation of the federal government's commitment to fighting cybercrime. The Order correctly identifies ransomware and cyber-enabled fraud as activities carried out by Transnational Criminal Organizations (TCOs)—many of which operate with the willing or tacit support of foreign regimes—and directs a coordinated, whole-of-government response.

Several elements of the Order are particularly significant. The directive to develop an action plan identifying specific TCOs and proposing solutions to prevent, disrupt, investigate, and dismantle them reflects the kind of targeted, intelligence-driven approach that has proven effective against other serious criminal enterprises. The creation of an operational cell within the National

Coordination Center to synchronize federal disruption efforts is a meaningful structural step. And the International Engagement provisions—which direct the Secretary of State to demand enforcement action from nations harboring cybercriminals and to coordinate sanctions, visa restrictions, and trade penalties with allies—address one of the core structural enablers of ransomware: the impunity enjoyed by criminals operating in permissive jurisdictions.

The new National Cyber Strategy reinforces this by elevating ransomware and cybercrime to top-tier national security threats and articulating six pillars for action. I was particularly encouraged by the Strategy's framing around shaping adversary behavior. The only way to address the societal, business, and technical threats posed by ransomware is to raise costs and inject uncertainty into criminal ecosystems at the same time that we put the technical tools in place to kick them off victim networks and slam the doors behind them.

The Executive Order and Strategy together create a strong policy foundation. Now we must build on it.

V. Using Existing Authorities in Novel Ways to Stop the Worst Actors

The federal government has more tools available than it is currently using at full force against the most dangerous ransomware actors. I want to highlight three areas where I believe existing authorities could be applied more aggressively and creatively, and where I urge this Committee to provide support and, where necessary, legislative clarification.

A. Terrorism Designations for Those Who Target Hospitals and Critical Infrastructure

The federal definition of terrorism under 18 U.S.C. § 2331 includes "violent acts or acts dangerous to human life" that "appear to be intended to intimidate or coerce a civilian population." Under 8 U.S.C. § 1182(a)(3)(b), terrorist activities include "seizing or detaining, and threatening to kill, injure, or continue to detain" a person "in order to compel a third person" to act as a condition for release.

When a ransomware gang encrypts a hospital's systems and demands payment under threat of continued system lockout—knowing that patients are being diverted, that dialysis is being delayed, that surgery schedules are being canceled—I believe a serious legal argument exists that this conduct falls within those definitions. At minimum, it merits a formal, deliberate analysis by the Departments of State, Justice, and Treasury, who collectively hold designation authority under Executive Order 13224.

I am not alone in this view. John Riggi, the National Advisor for Cybersecurity and Risk at the American Hospital Association, has testified before Congress that ransomware attacks targeting hospitals should be investigated with the same urgency as terrorism. The Director-General of the World Health Organization has briefed the UN Security Council that these attacks "at worst... cause patient harm and death." U.S. and French ambassadors at that same session emphasized the escalating harm.

I want to be direct about what terrorism designations would and would not accomplish. They are not a cure-all. They would not capture every ransomware actor. Nor should they. The deliberative designation process led by the State Department is designed precisely to ensure we act surgically. But for the most egregious actors—those who knowingly and repeatedly target hospitals, who have caused documented patient deaths, who operate at scale against the institutions that keep Americans alive—terrorism designations would unlock a powerful set of

additional tools: asset freezing, heightened Intelligence Community collection authorities, expanded travel restrictions, and significant diplomatic consequences for nations harboring these individuals.

We should also begin a national conversation—one I would urge this Committee to facilitate—about whether potential gaps in cyber insurance coverage caused by terrorism designation triggers could be addressed through the Terrorism Risk Insurance Act framework when Congress considers reauthorization in 2027. The goal is not to punish victims. It is to ensure that the most dangerous actors in the ransomware ecosystem face consequences proportionate to the harm they cause.

B. Murder and Manslaughter Charges Where Attacks Cause Death

Under federal law, the felony murder rule allows a defendant to be charged with first-degree murder when they commit a dangerous felony that results in another person's death, even if they did not cause the death directly. Under New York law, a defendant can be charged with second-degree murder when, "under circumstances evincing a depraved indifference to human life," they "recklessly engage[] in conduct which creates a grave risk of death to another person, and thereby cause[] the death of another person."

The University of Minnesota study I referenced earlier documented at least 47 deaths attributable to hospital ransomware attacks between 2016 and 2021. As ransomware attacks on healthcare have nearly doubled since that study's endpoint, the true number of lives lost to this crime is almost certainly in the hundreds. Federal prosecutors should be empowered—and encouraged—to evaluate whether homicide charges are appropriate in cases where ransomware actors targeted hospitals, where deaths resulted, and where the actors demonstrated clear foreknowledge that their actions endangered life.

This is not a theoretical exercise. Consider what happened just two months ago, on February 19, 2026, when ransomware actors struck the University of Mississippi Medical Center. UMMC is not simply a large hospital. It is the medical backbone of an entire state: Mississippi's only academic medical center, operating seven hospitals and 35 clinics statewide, and home to the state's only Level 1 trauma center, only children's hospital, and only organ and bone marrow transplant program. When attackers took down UMMC's network—knocking Epic, its electronic health records system, fully offline and forcing clinical staff to revert to pen and paper—they did not merely disrupt a business. They degraded the emergency medical capacity of an entire state. Clinics closed across Mississippi. Outpatient surgeries and cancer treatment appointments were canceled. For nine days, the state's only facility equipped to handle the most severe trauma cases operated under manual downtime procedures, with staff tracking patient care, medications, and orders on paper. Nearby hospitals reported surging emergency department volumes as they stepped in to absorb patients UMMC could not fully serve.

As the American Hospital Association's John Riggi noted in response to the attack, disruptions like this are especially dangerous in rural states where the next nearest trauma center may be over 100 miles away. The hackers behind the UMMC attack knew exactly what they were targeting. They contacted the hospital afterward with demands. They understood they had taken down a system that Mississippi patients depend on for survival—and they used that leverage deliberately.

Campbell County Health in Wyoming offers another instructive example: its entire hospital network was crippled for over two weeks, forcing emergency patients to be transferred across distances of 70 miles for eight hours while its single emergency department was offline. The link

between these interruptions and patient mortality is documented in the peer-reviewed literature. The Executive Order directs the Attorney General to pursue the "most serious, provable offenses" arising from cybercrime. Homicide charges in appropriate cases would be consistent with that directive—and would send a signal to ransomware actors that is long overdue.

C. Sanctions and Treasury Authorities Against Ransomware Financial Infrastructure

The ransomware economy depends on a financial infrastructure: cryptocurrency exchanges, money laundering networks, and payment processors that move ransom proceeds across borders. The Treasury Department's Office of Foreign Assets Control has used sanctions authority to designate ransomware actors and the exchanges that service them. I urge this Committee to support the expansion of that program, in alignment with the Executive Order's international engagement provisions.

Blockchain tracing by firms like TRM and Chainalysis shows that annual ransomware payments, while down from their 2023 peak, remain at well over $800 million. Disrupting the financial ecosystem that makes ransomware profitable—through expanded sanctions, cooperation with foreign financial intelligence units, and pressure on cryptocurrency infrastructure providers—remains one of the highest-leverage interventions available to the government. The International Counter Ransomware Initiative, now comprising over 60 nations, provides a ready-made multilateral framework for coordinating these actions.

VI. Recommendations for This Committee

I offer the following specific recommendations for this Committee's consideration:

- Direct the Departments of State, Justice, and Treasury to formally evaluate and report back to Congress on whether existing terrorism designation authorities under Executive Order 13224 can be applied to ransomware actors who knowingly target hospitals and critical life-safety infrastructure.
- Request a report from the Department of Justice on the feasibility and appropriateness of pursuing homicide charges in cases where ransomware attacks on healthcare facilities resulted in documented patient deaths.
- Encourage the Attorney General to issue guidance making clear that cyber-enabled attacks with life-safety consequences will be prosecuted using the most serious applicable charges, consistent with the directive in Executive Order 14390 to pursue the most serious provable offenses.
- Support the full funding and reauthorization of the State and Local Cybersecurity Grant Program. State and local governments are disproportionately targeted by ransomware, and they often lack the resources to defend themselves. Governments and government services was the fourth most targeted sector in 2025. Cutting this funding would be a gift to ransomware criminals.
- Convene a Congressional working group, including representatives from the insurance industry, to evaluate amendments to the Terrorism Risk Insurance Act ahead of its 2027 reauthorization that would address cyber terrorism, ensuring that terrorism designations for ransomware actors do not inadvertently harm victims who need insurance coverage to recover.

- Work with the National Security Council to ensure that federal cybersecurity experts are meaningfully integrated into the terrorism designation review process when ransomware actors targeting healthcare are under consideration.

VII. Conclusion

The people running ransomware organizations that target American hospitals are not mysterious hackers operating in a moral gray zone. They are criminals who have made deliberate choices. Choices to target the sick, the vulnerable, the elderly, and the newborn, because they have calculated that doing so maximizes their profits. They have no shame about this. They have demonstrated, repeatedly, that they will not stop unless we make stopping necessary.

The FBI and its federal partners are doing everything they can with the authorities they currently have. I know this from the years I spent working alongside those agents. But the worst of the worst—those targeting healthcare, those who have caused documented deaths, those operating with impunity under the protection of hostile foreign governments—deserve to face consequences that match the gravity of what they have done.

The President's Executive Order has given us a mandate. The National Cyber Strategy has given us a framework. This Committee has the power to sharpen both, fill the gaps, and send a message to the criminal ecosystem that America is no longer willing to treat ransomware as merely a cost of doing business in the digital age.

These hackers are counting on us to respond with incremental measures. I urge you to prove them wrong.

I thank the Subcommittees for this opportunity and look forward to your questions.

Cynthia Kaiser
Senior Vice President, Halcyon Ransomware Research Center
Former Deputy Assistant Director, FBI Cyber Division
Submitted: April 21, 2026