# The Ransomware Task Force Report at Five Years

*Note: The following excerpt is taken from testimony of Megan Stifel on April 21, 2026 in front of the House Committee on Homeland Security's Subcommittees on Border Security and Enforcement and Cybersecurity and Infrastructure Protection for a hearing titled "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans." The full testimony is available here.*

Released in April 2021, the Ransomware Task Force (RTF) Report is a seminal document that provides actionable recommendations for combating cybercrime across four phases: Deter, Detect, Prepare, and Respond. With participation from across government, industry, and civil society, RTF outputs have informed U.S. and international policy making and have served as a blueprint for private sector actors aiming to protect themselves from transnational criminal organizations.

As we mark the five-year anniversary of the release of the RTF report and its 48 recommendations, we have several observations:

» **There's been significant progress, but it has slowed**. Since our last assessment of progress against the RTF recommendations,[1] two have moved from preliminary action to significant action. Specifically, the insurance industry has seen progress through consortia like CyberAcuView,[2] which is making it easier to understand claims data in aggregate (Recommendation 2.1.7). The government also continues to map the ransomware ecosystem, including supporting infrastructure, and is now regularly using this knowledge to inform takedowns and sanction activities.

» **Several recommendations await final action by the government**. Implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), championed by many members of this committee, remains stalled more than four years after its passage (Recommendations 4.2.2, 4.2.3, and 4.2.4).[3] With a final CIRCIA rule in place, we would have a better operational understanding of the ransomware ecosystem and the ability to more easily offer assistance to victims.

» **For the first time, we've seen backsliding**. Since our assessment in April 2024, two of our recommendations have moved from significant action back to preliminary action. Notably for this committee, the failure to fund the state and local cyber grant program since its original appropriation lapsed last year leaves governments at significant risk from ransomware and other

1 https://securityandtechnology.org/wp-content/uploads/2024/10/April-2024-RTF-Progress-Report-Doubling-Down.pdf

2 https://cyberacuview.com/

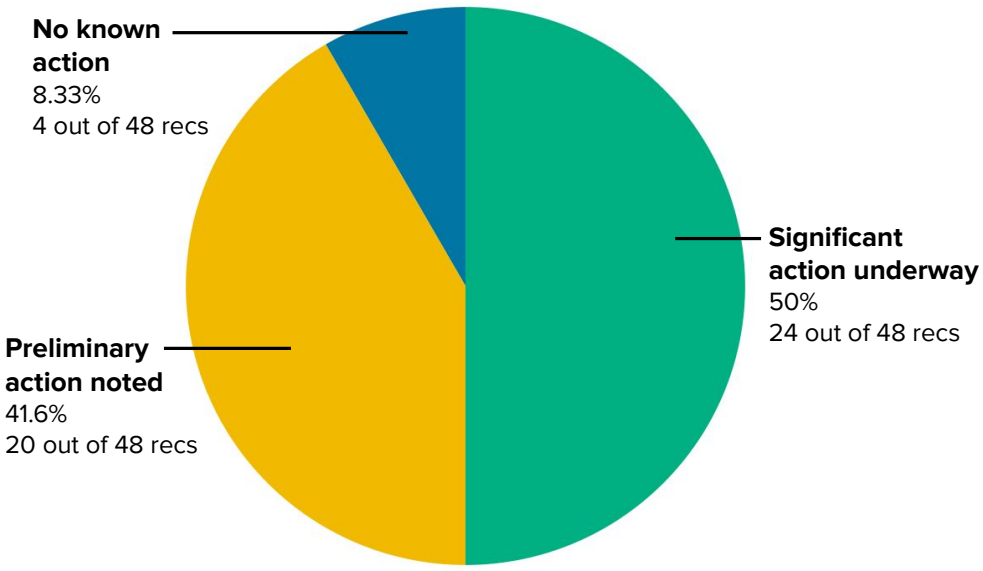
3 https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings

cyber intrusions (Recommendation 3.4.2).[4] While this committee has made strides in advancing a long-term reauthorization of the grant program,[5] without funding, states will remain exposed. The Cyber Response and Recovery Fund, authorized in 2021 in response to RTF recommendations, may also be at risk; the January House-passed Homeland Security appropriations bill would have transferred all of the money from this emergency account to base CISA appropriations (Recommendation 4.1.1).[6]

» **Limitations on ransom payments remain underdeveloped**. Of the four RTF recommendations where we have seen no action, three pertain to pre-ransom payment activities, such as conducting a cost-benefit analysis (Recommendation 4.3.2). The record-low ransom rates may open up space for more conversations on how to limit payments, which are the fuel for the entire ecosystem. However, absent strong leadership from policymakers to act as a catalyst, we are unlikely to see significant progress.

On balance, the success of RTF members and partners in implementing recommendations has had a significant impact on the ransomware ecosystem, including driving criminals to pursue alternative, non-encryption-based extortion methods. Key to our approach was starting with a comprehensive strategy that addresses all phases of the challenge and providing clear recommendations to specific actors. We also favored system-level approaches that affect the root causes of cybercrime, rather than trying to treat its symptoms. Finally, we could not have succeeded without deep collaboration with industry. Civil society organizations like IST have a vital role to play as a neutral convener and accelerant to policy engineering projects; however, effectuating real and lasting change requires bringing both government and industry perspectives to the table.

## Chart: Progress on RTF Recommendations as of April 2026




4 https://www.nascio.org/wp-content/uploads/2026/02/NASCIO-Advocacy-Priorities-2026_a11y_SLCGP.pdf

5 https://www.congress.gov/bill/119th-congress/house-bill/5078

6 https://docs.house.gov/billsthisweek/20260119/Homeland26_01_xml.pdf

# GOAL 1: DETER RANSOMWARE ATTACKS

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Signal that ransomware is an international diplomatic and enforcement priority | 1.1.1 | Issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority. | |
| | 1.1.2 | Establish an international coalition to combat ransomware criminals. | |
| | 1.1.3 | Create a global network of ransomware investigation hubs. | |
| | 1.1.4 | Convey the international priority of collective action on ransomware via sustained communications by national leaders. | |
| Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House | 1.2.1 | Establish an Interagency Working Group for ransomware. | |
| | 1.2.2 | Establish an operationally focused U.S. government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub. | |
| | 1.2.3 | Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign. | |
| | 1.2.4 | Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public. | |
| | 1.2.5 | Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat. | |
| | 1.2.6 | Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns. | |
| Substantially reduce safe havens where ransomware actors currently operate with impunity | 1.3.1 | Exert pressure on nations that are complicit or refuse to take action. | |
| | 1.3.2 | Incentivize cooperation and proactive action in resource-constrained countries. | |

# GOAL 2: DISRUPT THE RANSOMWARE BUSINESS MODEL

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Disrupt the system that facilitates the payment of ransoms | 2.1.1 | Develop new levers for voluntary sharing of cryptocurrency payment indicators. | |
| | 2.1.2 | Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws. | |
| | 2.1.3 | Incentivize voluntary information sharing between cryptocurrency entities and law enforcement | |
| | 2.1.4 | Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes. | |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Disrupt the system that facilitates the payment of ransoms | 2.1.5 | Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation. | |
| | 2.1.6 | Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs. | |
| | 2.1.7 | Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management. | Significant action underway. The insurance industry has seen progress through consortia like CyberAcuView, which is making it easier to understand claims data in aggregate. |
| Target the infrastructure used by ransomware criminals | 2.2.1 | Leverage the global network of ransomware investigation hubs. | |
| | 2.2.2 | Clarify lawful defensive measures that private-sector actors can take when countering ransomware. | |
| Substantially reduce safe havens where ransomware actors currently operate with impunity | 2.3.1 | Increase government sharing of ransomware intelligence. | |
| | 2.3.2 | Create target decks of ransomware developers, criminal affiliates, and ransomware variants. | Significant action underway. Recent takedown activity has targeted ransomware-as-a-service and the entire ecosystem, in coordination with industry and international partners. |
| | 2.3.3 | Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure. | |

# GOAL 3: HELP ORGANIZATIONS PREPARE

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Support organizations with developing practical operational capabilities | 3.1.1 | Develop a clear, actionable framework for ransomware mitigation, response, and recovery. | |
| | 3.1.2 | Develop complementary materials to support widespread adoption of the Ransomware Framework. | |
| | 3.1.3 | Highlight available internet resources to decrease confusion and complexity. | |
| Increase knowledge and prioritization among organizational leaders | 3.2.1 | Develop business-level materials oriented toward organizational leaders. | |
| | 3.2.2 | Run nationwide, government- backed awareness campaigns and tabletop exercises. | |
| Update existing, or introduce new, cybersecurity regulations to address ransomware | 3.3.1 | Update cyber-hygiene regulations and standards. | |
| | 3.3.2 | Require local governments to adopt limited baseline security measures. | |
| | 3.3.3 | Require managed service providers to adopt and provide baseline security measures. | |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Financially incentivize adoption of ransomware mitigations | 3.4.1 | Highlight ransomware as a priority in existing funding provisions. | |
| | 3.4.2 | Expand Homeland Security Preparedness Grants to encompass cybersecurity threats. | Reversal of significant progress. The State and Local Cybersecurity Grant Program is currently defunded. |
| Financially incentivize adoption of ransomware mitigations | 3.4.3 | Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework. | |
| | 3.4.4 | Alleviate fines for critical infrastructure entities that align with the Ransomware Framework. | |
| | 3.4.5 | Investigate tax breaks as an incentive for organizations to adopt secure IT services. | |

# GOAL 4: RESPOND TO RANSOMWARE ATTACKS

| Objective | Rec. | Description | Change since April 2024? |
|---|---|---|---|
| Increase support for ransomware victims | 4.1.1 | Create ransomware emergency response authorities. | |
| | 4.1.2 | Create a Ransomware Response Fund to support victims in refusing to make ransomware payments. | |
| | 4.1.3 | Increase government resources available to help the private sector respond to ransomware attacks. | |
| | 4.1.4 | Clarify United States Treasury guidance regarding ransomware payments. | |
| Increase the quality and volume of information about ransomware incidents | 4.2.1 | Establish a Ransomware Incident Response Network (RIRN). | Reversal of significant progress. The RIRN is defunct, and there is still inconsistent sharing of incident reports across jurisdictions. However, agreements like the initiative between the Department of Homeland Security and DG Connect are indicators of preliminary action aligned with this recommendation. |
| | 4.2.2 | Create a standard format for ransomware incident reporting. | |
| | 4.2.3 | Encourage organizations to report ransomware incidents. | |
| | 4.2.4 | Require organizations and incident response entities to share ransomware payment information with a national government prior to payment. | |
| Require organizations to consider alternatives to paying ransoms | 4.3.1 | Require organizations to review alternatives before making payments. | |
| | 4.3.2 | Require organizations to conduct a cost-benefit assessment prior to making a ransom payment. | |
| | 4.3.3 | Develop a standard cost-benefit analysis matrix. | |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION