**David J. Kappos**
+1-212-474-1168
dkappos@cravath.com

**Timothy G. Cameron**
+1-212-474-1120
tcameron@cravath.com

**John D. Buretta**
+1-212-474-1260
jburetta@cravath.com

**David M. Stuart**
+1-212-474-1519
dstuart@cravath.com

**David L. Portilla**
+1-212-474-1410
dportilla@cravath.com

**Evan Norris**
+1-212-474-1524
enorris@cravath.com

**Michael L. Arnold**
+1-212-474-1664
marnold@cravath.com

# White House Open Letter Warns Companies of Ransomware Threat

*June 10, 2021*

On June 2, 2021, following weeks of reports of ransomware attacks impacting U.S. and global businesses, the White House issued an open letter warning of the acute threat posed by such attacks and urging companies to take immediate steps to protect their core business operations. Issued by the National Security Council's top cyber official, the open letter comes on the heels of the President's May 12, 2021 Executive Order *Improving the Nation's Cybersecurity*, which focuses on measures to bolster the security of public sector networks and incident response. The unusual letter encourages companies to voluntarily adopt the same set of best practices the Executive Order imposes on federal government agencies and contractors and reflects the degree to which the new Administration views cybersecurity as critical both to U.S. national and economic security.

The White House open letter follows the publication of multiple advisories to the business community addressing ransomware-related compliance risks issued over the past year by U.S. regulatory agencies, including the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and Financial Crimes Enforcement Network ("FinCEN"), as well as the U.S. Securities and Exchange Commission ("SEC"). In light of the current threat environment and the important role of advanced planning for corporations, financial institutions and other organizations to successfully to defend against ransomware attacks, we write to summarize the guidance issued by the White House and U.S. financial regulators.

## WHITE HOUSE OPEN LETTER

### Purpose and Scope

Addressed to "Corporate Executives and Business Leaders", the White House open letter starkly describes the threat arising from the recent increase in the number and size of ransomware attacks across the globe:

> Ransomware attacks have disrupted organizations around the world, from hospitals across Ireland, Germany and France, to pipelines in the United States and banks in the U.K. The threats are serious and they are increasing.

The letter emphasizes that any company - regardless of size, location, industry or sophistication - may find itself victim of a ransomware attack and asserts that a "key takeaway" from the recent attacks is that "companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively." The letter notes the work U.S. law enforcement agencies and their partners are doing to disrupt and deter ransomware actors but also emphasizes the "critical responsibility" the private sector has with respect to protecting their customers and the broader U.S. economy against ransomware threats.

### Guidance for the Private Sector

The open letter sets forth a list of measures the White House urges companies to implement immediately to protect against the risk of a ransomware attack. Among these are several "high impact" best practices: the use of multifactor log-in authentication, endpoint detection and response to locate and block malicious activity, encryption to prevent the use of stolen data and employment of a skilled and empowered security team to rapidly respond to threats.

In addition, the open letter encourages companies to take a number of other steps on an urgent basis:

- *Backups*. Company data, system images and configurations should be regularly backed up, tested and kept offline. As ransomware actors frequently try to find and encrypt accessible backups, ensuring that backed-up data is not connected to the company's business network is vital.
- *Update and patch*. Companies should timely update and maintain the security of their operating systems, applications and firmware and consider centralizing their patch management systems.
- *Testing*. Companies should conduct exercises to test their incident response plans, with a focus on assessing their ability to maintain core business operations without access to compromised systems. Companies should also use third parties to conduct penetration testing of their cybersecurity systems to further assess the ability of their security team to defend against a sophisticated attack.
- *Network segmentation*. As ransomware attacks become more focused on disrupting operations rather than stealing data, companies should focus on ensuring business functions and manufacturing/production operations are separated onto different networks. Links between networks, and access to mission-critical networks, should be carefully limited and monitored.

The open letter ends by encouraging the private sector to take the steps outlined and promising that the U.S. government will do its part to increase efforts to hold the groups who commit ransomware attacks accountable.

## OTHER U.S. GOVERNMENT ADVISORIES

The White House open letter adds to the growing collection of guidance documents and advisories issued in the past year by U.S. regulatory agencies, including OFAC, FinCEN and the SEC, to address the ransomware threat.

### OFAC Advisory on Sanctions Risks for Facilitating Ransomware Payments

On October 1, 2020, OFAC issued an advisory to highlight the sanctions risks associated with payments – typically in digital currency – related to ransomware attacks, which is significant both for companies that may fall victim to such attacks, as well as for the financial institutions, cyber insurance companies and incident response firms that may facilitate payments on their behalf. The advisory notes that OFAC has designated numerous cyber actors through its sanctions programs and explains that ransomware payments made to designated or blocked persons, or with a nexus to a comprehensively sanctioned jurisdiction, may result in a sanctions violation by the company making or facilitating the payment. At the same time, the advisory notes that a company's self-reporting of a ransomware attack, along with cooperation more generally, will be viewed by OFAC as a significant mitigating factor in the event a payment with a sanctions nexus is ultimately made and the agency must evaluate the potential enforcement consequences.

### FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Also issued on October 1, 2020, FinCEN's advisory addresses the ways in which ransomware payments may implicate the Bank Secrecy Act and anti-money laundering regime in the event a payment to a ransomware actor utilizes the U.S. banking system. The advisory notes that financial institutions should consider whether a suspicious activity report ("SAR") is required when dealing with a ransomware payment that is made by, at or through the financial institution. The advisory also identifies several "red flag indicators" for financial institutions that may be signs of suspicious transactions associated with ransomware attacks, such as transactions between organizations that are at particularly high risk of suffering an attack (*e.g.*, government, financial, educational, healthcare) and the digital forensics and incident

response firms and cyber insurance companies that facilitate ransomware payments. The FinCEN advisory is significant for all financial institutions and firms that facilitate ransomware payments, and, among other things, makes clear that companies considering making a ransomware payment should anticipate that a SAR will be filed.

**SEC Risk Alert on Cybersecurity: Ransomware Alert**

On July 10, 2020, the SEC's Office of Compliance Inspections and Examinations issued a risk alert regarding the increase in sophistication of ransomware attacks on SEC registrants, including broker-dealers, investment advisers and investment companies. The alert encourages registrants to consider strengthening their cybersecurity defenses in ways similar to those expressed in even stronger terms in this month's White House open letter. The alert also serves to further highlight the attention the Commission has paid in the last several years to a range of cybersecurity issues applicable not just to financial services firms but to all public companies, including disclosure of material risks and incidents, customer data protection and compliance. In addition to the risks discussed above, companies considering the compliance risks posed by a ransomware attack thus must also be mindful that such an attack may lead to scrutiny from the SEC regarding the sufficiency of their disclosures and of their policies, practices and procedures with respect to cybersecurity preparedness and resiliency.

## CONCLUSION

The White House open letter underscores the degree to which the threat of a ransomware attack has sharply increased in recent weeks and the potential impact on core operations when a business fails to adequately prepare for an attack. At the same time, the advisories issued by U.S. government financial regulators make clear that businesses that fall victim to such an attack must be attuned to a range of immediate and longer-term compliance risks even as they seek to mitigate the attack's most harmful impacts. As the threat posed by ransomware and other cyber attacks continues to grow and evolve, we encourage clients continually to review their cybersecurity defenses and incident response plans. Should you have questions related to the issues covered in this memorandum, please do not hesitate to contact any one of us.



**New York**
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

**London**
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com