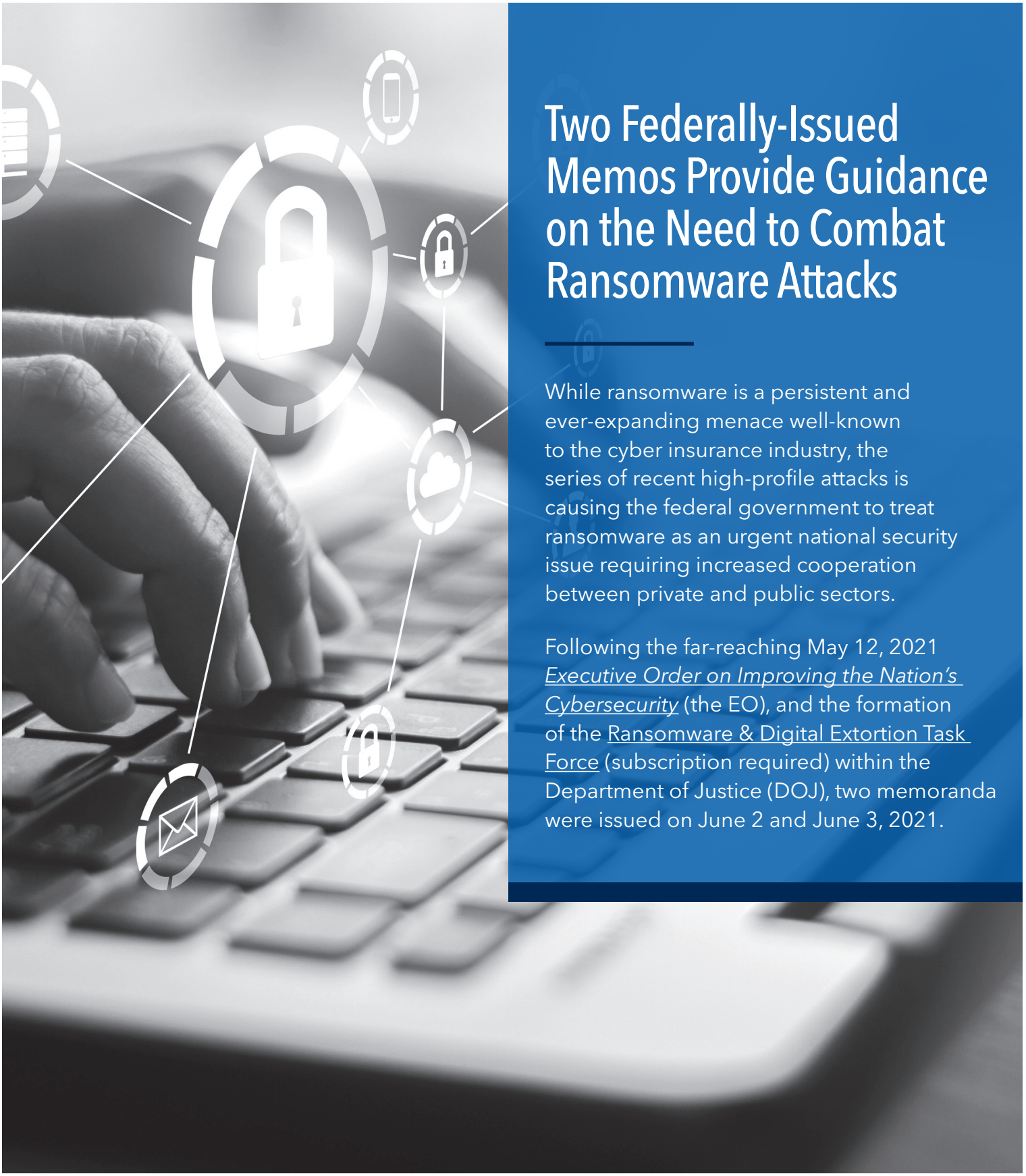

Two Federally-Issued Memos Provide Guidance on the Need to Combat Ransomware Attacks

While ransomware is a persistent and ever-expanding menace well-known to the cyber insurance industry, the series of recent high-profile attacks is causing the federal government to treat ransomware as an urgent national security issue requiring increased cooperation between private and public sectors.

Following the far-reaching May 12, 2021 *Executive Order on Improving the Nation's Cybersecurity* (the EO), and the formation of the Ransomware & Digital Extortion Task Force (subscription required) within the Department of Justice (DOJ), two memoranda were issued on June 2 and June 3, 2021.

CONNER STRONG & BUCKELEW

MULLEN COUGHLIN

Edward Cooney
Conner Strong & Buckelew
Vice President, Account Executive
973-659-6424

On June 2nd, the White House issued a memorandum to corporate executive and business leaders urging them to take a number of precautions to prevent ransomware and protect their companies' assets. The next day, Deputy Attorney General (AG) Lisa Monaco issued a memorandum to federal prosecutors outlining guidance for investigating ransomware and digital extortion issues.

The June 2nd Memorandum outlined the following (fairly standard) concrete actions for businesses to take:

- Implement the best practices from President Biden's May 12, 2021 *Executive Order on Improving the Nation's Cybersecurity*;
- Enable Multifactor Authentication (MFA) because passwords are routinely compromised;
- Utilize Endpoint Detection and Response (EDR) to hunt for malicious activity on a network and block it;
- Encrypt data so, if it is stolen, it is rendered unusable;
- Employ a skilled and empowered security team to patch rapidly and incorporate threat information in the organization's defenses;
- Backup data, system images and configurations, and
  - Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups;
- Update and patch systems, including operating systems, applications and firmware, promptly by using a centralized patch management system governed by a risk-based assessment strategy;
- Build and test the organization's incident response plan;
- Use third-party penetration testing to evaluate the security and defensibility of the organization's systems;
- Segment the networks that control corporate business functions and manufacturing/production operations so that industrial control system networks can continue operating if the corporate network is compromised, and
  - Filter and limit internet access to operational networks and identify links between the networks; and
- Regularly test contingency plans, such as manual controls or workarounds, so that safety critical functions can be maintained during a cyber incident.

On June 2nd, the White House issued a memorandum to corporate executive and business leaders urging them to take a number of precautions to prevent ransomware and protect their companies' assets.

The White House also recommends that business executives convene their leadership teams to discuss the growing ransomware threat to core business operations, review corporate security posture and business continuity plans and ensure that the organization has the ability to continue or quickly restore operations.

While the federal government is strengthening its efforts to stop ransomware attacks by disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing of virtual currency proceeds, the White House urged the private sector to take responsibility to protect themselves against cyber threats and stated that no company or industry is safe from being targeted.

The June 3rd Memorandum from Deputy AG Lisa Monaco laid out existing DOJ requirements, as well as new requirements, for all DOJ investigations and cases that involve ransomware and digital extortion. These include the following:

- The assigned Assistant United States Attorney must notify the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ and the National Security & Cyber Crime Coordinator (Coordinator) for the Executive Office for United States Attorneys (EOUSA) when an investigation is opened or there is a significant new development in an investigation;
- The CCIPS and Coordinator must be notified any time a U.S. Attorney's Office learns of a ransomware or digital extortion attack in its District, regardless of whether it implicates an open matter, and

- An "Urgent Report" must be issued by the U.S. Attorney's Office of any new ransomware or digital extortion attack in its District and for other delineated triggers; and

- The CCIPS must coordinate responses and track and monitor all ongoing developments in these matters.

Both memoranda advance the theme outlined by the EO – that increased reporting, tracking, coordination and cyber defenses are necessary to combat the ransomware threat.

The flurry of recent federal government activity is a welcome sign to those in the cyber defense and cyber insurance industry who have been dealing with the increased human and monetary cost of ransomware and digital extortion for years. Businesses and consumers, many of whom have been victims of ransomware and data theft, should also welcome the increased role being undertaken by the federal government.

About Mullen Coughlin

Mullen Coughlin is the largest team of experienced attorneys uniquely focused on providing tailored data privacy and incident response services, including breach response, pre-breach planning and compliance, regulatory investigation and management, and privacy litigation defense under the umbrella of cyber insurance. Conner Strong & Buckelew partners with Mullen Coughlin in providing incident response to our clients under Cyber Insurance Policies.

About Conner Strong & Buckelew

Conner Strong & Buckelew is among America's largest insurance brokerage, risk management and employee benefits brokerage and consulting firms. The firm is an industry leader in providing high-risk businesses with comprehensive solutions to prevent losses, manage claims, and drive bottom line growth. Its employee benefits practice focuses on providing best-in-class benefits administration, health and wellness programs and strategic advisory services.

The company provides insurance and risk services to a wide-range of industries including but not limited to aviation, construction, education, healthcare, hospitality & gaming, life science & technology, public entity and real estate. Additionally, Conner Strong & Buckelew and its affiliates offer a number of innovative and specialty solutions which include captive strategies, construction wrap-ups, executive risk, safety and risk control, and private client services.

Founded in 1959 with offices in New York, New Jersey, Pennsylvania, Georgia, Massachusetts, Florida, and Delaware, Conner Strong & Buckelew has a team of nearly 450 professionals, serving clients throughout the United States and abroad.

CONNER STRONG & BUCKELEW

MULLEN COUGHLIN