CYBERSECURITY:

The Evolving Threats and Challenges for the Construction Industry and Government Contractors

B. Stephanie Siegmann, Partner, Hinckley Allen
Alex Trafton, Managing Director, Ankura

This is for informational purposes only and is not intended to be legal advice.

Table of Contents:

I. Introduction

The cyberthreat environment continues to grow more menacing. Over the last year, organizations have been faced with a weekly, if not daily, deluge of ominous cybersecurity alerts and advisories from law enforcement. Cyberattacks come in many forms – *i.e.,* malware-based attacks, phishing, spoofing, zero-day exploits, denial-of-service attacks, supply chain attacks, and insider threats, among others – and are clearly on the rise. No organization is immune. Indeed, over the last year, the vast majority of companies experienced some form of a cyberattack.[1] Accordingly, it is not matter of *if* your organization will experience a cyberattack but *when*, and what you can do to minimize liability risks. This article 1) details the growing threats posed by cybercriminals; 2) describes Business Email Compromise ("BEC") and Ransomware attacks; 3) highlights the latest developments in cybersecurity regulations and compliance; 4) discusses the increased enforcement landscape on cybersecurity compliance; 5) analyzes the impact of the Supreme Court's recent False Claims Act decision and; 6) provides tips to avoid becoming a target of a federal or state enforcement action.

II. The Cyber Threat Environment

Government contractors are witnessing a rapidly evolving cyber regulation landscape. These changes have been driven by the U.S. Government's attempt to counter the growing cyber threats from both strategic adversarial nations as well as cyber criminals. Over the last 20 years, U.S. Government cyber regulations have grown more comprehensive and stringent in direct response to high-profile cyber-attacks, with each attack seemingly prompting a statutory and/or regulatory response from either the Legislative or Executive Branch. The most significant of these attacks included the Office of Personnel Management ("OPM") hack, the Microsoft Exchange hack, and the SolarWinds hack, all of which targeted U.S. government agencies and government contractors (that is, companies in the private sector, which provided products and services to federal agencies). Most recently, a Russian extortion gang called CLoP stole the personal data of more than 60 million individuals from approximately 600 organizations, including government agencies, by exploiting a vulnerability in MOVEit, a file transfer program and a Chinese state-backed hacking group,

Storm-0558, hacked into the email accounts of 25 organizations, including unclassified emails of senior members of the U.S. Departments of Commerce and State, using an extremely sophisticated method – leveraging a flaw in a Microsoft cloud-computing environment (i.e., a validation error in Microsoft code).

In addition to attacks targeting federal government agencies and their supply chains, business organizations of all types and sizes face ever growing threats from cyber-attacks. The cost of intellectual property theft is staggering. Intellectual property theft has cost the U.S. economy $200 to $600 billion per year. Much of this theft results from national state cyber-attacks. These cyber-attacks represent not only an immediate threat to the national security of the United States, but also long-term erosion of U.S. competitive advantage in the global economy.

As cyber-attacks differ in type and target, so do the threat actors perpetrating these attacks. Cyber threat actors can be categorized by both their motivations as well as their capabilities. Below is a non-exhaustive list of cyber threat actors grouped by both motivation and capability:

Advanced Persistent Threats ("APTs") – Well-resourced threat actors, typically these actors are operating on behalf of or sponsored by a nation state. APTs typically lie in wait after network intrusion for some time, obscuring their activities while they conduct data exfiltration or other malicious activities.

Cybercriminals / Organized Crime – These may be lone actors or groups of actors who engage in cyber-attacks for the purpose of financial gain. Cybercriminals tend to exploit vulnerabilities more rapidly to capitalize on their intrusion; this can include ransomware or intellectual property theft.

Hacktivists – Threat actors who engage in cyber-attacks for ideological purposes. Hacktivists tend to favor vandalizing or exploiting high-profile targets to convey ideological messages.

Script Kiddies – Less skilled or sophisticated threat actors who lack the ability to design and customize cyber intrusion tools, but who may use tools developed by other attackers to penetrate a network or system.

Insiders – While many perceive cyberattacks as the tool of external threat actors, often insiders are the cause of a compromise. These may be intentional attacks or simply accidental disruptions or compromises to organizational systems. Insiders often pose the greatest risk as they are authorized users of the organization's systems.

While any of the above actors could compromise a system or network, APTs present the greatest risk to U.S. critical infrastructure and sensitive data. The People's Republic China ("PRC" or "China") and Russia pose the most acute cyberthreats to the United States. Due to emerging geopolitical issues as well as the increasing sophistication of both nations, the U.S. finds itself currently embroiled in a cyber cold war on two fronts.

A. China

The Office of the Director of National Intelligence's ("ODNI's") 2023 Annual Threat Assessment identified China as representing the "broadest, most active, and persistent cyber espionage threat to the U.S. Government and private-sector networks."[2] To illustrate the scope of this threat, U.S. Governmental Agencies have issued numerous public advisories concerning cyberespionage activities directed by the PRC government. In June 2023, the United States and international cybersecurity authorities issued a joint Cybersecurity Advisory concerning the significant threat posed by a PRC state-sponsored cyber actor, known as Volt Typhoon, to U.S. critical infrastructure sectors and other similar sectors worldwide using sophisticated tactics and techniques to evade detection.[3] Further, as noted above, Storm-055, Chinese-based hackers believed to be affiliated with the PRC government, secretly accessed email accounts of 25 organizations, including the accounts of U.S. Commerce Secretary Gina Raimondo, U.S. envoy to China, Nicholas Burns, and the U.S. Department of State's Assistant Secretary for East Asia, Daniel Kritenbrink, from May to June 2023.[4]

China has become the second largest world economy. As a result, the U.S. and China are now in natural competition, with the U.S.-China opposition becoming the defining rivalry of the 21st Century. The combination of tensions around Taiwan, China's "no-limits" policy with Russia during the Ukraine invasion, China's desire to use industrial espionage to close the technology gap with the U.S., and the tightening of U.S. trade controls focused on China,

have led to increasing cyber threats from the PRC. Most recently, reports that China is planning to establish a military training facility in Cuba has sparked alarm among security and intelligence officials, especially after PRC spy balloons were allowed to traverse across the United States.[5] If Cuba allows this military expansion, the PRC will have troops stationed less than one hundred miles from the Florida coast. China has operated intelligence collection facilities in Cuba since 2019.[6]

Since 2021, Zero Day attacks[7] have spiked. In September 2021, the Cyberspace Administration of China ("CAC") implemented new vulnerability reporting rules which require persons and entities to report discovered vulnerabilities to the Chinese government prior to reporting them to vendors. Microsoft has accused the Chinese government of exploiting these rules to accumulate a cache of Zero Day exploits which it can strategically deploy against critical targets in U.S. (and other) public and private entities. If true, this first of its kind vulnerability reporting rule creates an enormous advantage for Chinese APTs as they seek to compromise U.S. government and other critical infrastructure systems.[8]

China has also adopted a new counterespionage law, which went into effect on July 1, 2023, that significantly broadens the definition of spying increasing the risk of penalties being imposed against U.S. companies operating in China for what is considered "traditional business activities."[9] This law may be used to compel U.S. companies to assist the PRC government with its intelligence collection efforts against the United States. For instance, it "gives the [Chinese] Ministry of State Security and its local counterparts unprecedented enforcement powers to enter, question, [and] inspect individuals' electronic devices and business facilities."[10] This law could consequently assist China in "gather[ing] sensitive data from foreign firms under the guise of preventing espionage."[11] Such information could then be used to launch cyberattacks or assist China in developing political or military strategies detrimental to America.

B. Russia

The historical U.S.-Russia kinetic military rivalry has evolved due to the collapse of the Soviet Union and the emerging reliance on computer networks to accomplish both state and private industry functions. Russian cyber threat activity has principally been focused on its neighbors Ukraine, Estonia, and Georgia who had, in the opinion of Moscow, grown too

close to NATO and western countries. While Russia conducted cyberattacks and anti-democratic influence operations against all three nations, the most devastating attack was carried out using the "NotPetya" malware to cripple multiple Ukrainian public and private entities in 2017.[12] In addition to Russia's escalation of both its kinetic and cyber-attacks against its neighbors, it has also become more overtly aggressive towards the U.S. in its cyber intrusions, including direct interference in the 2016 U.S. elections and the 2020 SolarWinds hack. Russian hackers were responsible for creating both the Dark Energy 3 and NotPetya malware; the latter wreaked havoc, globally crippling the global shipping company Maersk and infecting U.S. companies, including those in the critical infrastructure sector, and causing massive damages. For example, thousands of Merck computers were damaged as a result of Russia's NotPetya malware attack resulting in losses of $1.4 billion. The malware had entered the company's systems through accounting software.

Russia's unprovoked 2022 invasion of Ukraine saw a new Russian warfare playbook, which incorporated a multi-domain assault blending traditional kinetic military operations with advanced cyber-attacks and influence operations designed to destabilize critical infrastructure as well as damaging confidence in western democratic institutions. While Russian military operations experience differing levels of success in Ukraine, Russian APTs continue to carry out attacks on western counties and infrastructure.

III. BEC Attacks

BEC attacks are one of most prolific and financially damaging cybercrimes. While phishing[13] remains the largest threat, the FBI found that BEC attacks make up more than one-quarter of all cybercrime losses and accounted for losses of over $2.7 billion in 2022.[14] Between 2016 and 2021, there were more than 240,000 BEC incidents and since 2016, BEC scams have resulted in more than $43 billion in losses globally. These scams are frequently carried out after compromising a legitimate business email account through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. The fraudster sends an email that fraudulently directs funds to a criminal-controlled account. The victim is tricked into believing that this email is from a trusted person – their boss or a corporate official, or trusted entity with whom they are doing business – and

transfers the money as instructed. Although they typically employ a low-tech social engineering scheme, these attacks can have devastating consequences for their victims. BEC fraudsters have become more sophisticated and their schemes have evolved from "simple hacking or spoofing of business and personal email accounts and a request to send wire payments to fraudulent bank accounts" to "utilizing custodial accounts held at financial institutions for cryptocurrency exchanges, or having victims send funds directly to cryptocurrency platforms where funds are quickly dispersed."[15] Indeed, North Korea's hackers have become increasingly sophisticated in their social engineering attacks, and BEC scams have raked in more than $3 billion in stolen cryptocurrency. The revenue from these BEC scams have been used to fund North Korea's nuclear weapons program.[16]

The real estate industry has been particularly vulnerable to BEC attacks. In 2021, members of the real estate industry were identified as the most common victim of impersonation using BEC schemes resulting in $6.9 billion in losses.[17] The attackers impersonate a party involved in a real estate transaction in email communications. Frequently, they pose as the seller's attorney or broker in email communications with an agent for the buyer and provide instructions to change a payment type or location to a fraudulent account. Once the funds are deposited, the cybercriminals withdraw the money from the fraudulent account making recovery difficult. Therefore, time is of the essence. Accordingly, it is imperative to report any suspected cybercrime immediately to the bank and FBI at www.ic3.gov so the funds can be frozen before the cybercriminals can withdraw the money resulting from the misdirected wire transfers.

There are steps businesses can take to protect themselves from BEC schemes. For instance, if an employee receives any financial account and address changes via e-mail or text message, the employee should follow up by calling the supplier, vendor, or contact person to verify the request was legitimate using only the phone number on record or on file. It is best to never use a contact number included in a fabricated email. Procedures should be put in place to verify payment and purchase requests outside of e-mail communication, including secure portals or direct phone calls to known verified numbers. Additionally, employees should be instructed not to bypass normal payment channels or procedures and not to respond to urgent payment requests that are out of the ordinary.

Further, employees should be provided frequent training on the importance of carefully examining e-mail addresses (especially from unknown senders), the URL, and spelling used in any correspondence and not to click on anything in an unsolicited email or text message. With the advancements in generative artificial intelligence, organizations should expect to see phishing emails and BEC scams that are far harder to detect as malicious. As a result, it is often best practice for organizations to institute geographic email restrictions to block sanctioned countries and overseas locations in which you do not engage in business. Moreover, these threats, like those from ransomware attacks described below, demonstrate the importance of implementing two-factor or multi-factor authentication to provide an additional and essential layer of security.

IV. Ransomware

While cyber threats vary, one of the most serious and persistent threats involves the use of ransomware to encrypt victim data and extort a ransom for its release. Ransomware attacks have significantly increased in the first six months of 2023 with threat actors having extorted more than $175 million than last year. 2023 is on pace to become one of the worst years in terms of ransomware payments.

Ransomware attacks have grown more sophisticated and aggressive, incorporating a significant number of new ransomware variants. Cybercrime has become increasingly lucrative and Ransomware-as-a-Service ("RaaS") is extremely popular on the dark web. RaaS is a criminal business model that makes it easy for anyone to execute a ransomware campaign and involves different groups of cyber actors in charge of the various steps of the attack. Typically, access brokers illegally obtain access to a network that they sell to a ransomware affiliate such as LockBit or BlackCat (a/k/a ALPHV). The ransomware affiliate then exfiltrates data from the victim's network and deploys ransomware, a form of malware, which they either buy or rent from the ransomware developers, to execute the ransomware attack. The ransomware affiliate leaves a ransom note on the encrypted network and has members that are involved in the ransom negotiation. If the victim pays the ransom, the ransomware affiliate has a customer support component that is available to assist the victim organizations with any problems decrypting the encrypted data. If the victim refuses to pay

the ransom, the ransomware affiliate offers to sell the data stolen from the victim network on a leak site on the dark web. Increasingly, these groups are publicly shaming their victims and even reaching out to the victim's customers to tell them that their data was stolen so as to increase the pressure on victims to pay.

The high-pressure tactics of ransomware gangs employ double extortion. After gaining access to a network, typically using compromised credentials or unpatched vulnerabilities, ransomware attackers move across a network looking for the most valuable data (often containing personally identifiable information or proprietary information), exfiltrate that data, and encrypt the compromised network using ransomware. Then, the attackers demand an exorbitant ransom for the decryption key so the victim can access their files and threaten to post or sell the stolen data, thereby exerting additional pressure to pay the ransom. The ransomware gangs use leak sites on the dark web to sell the victim's data and publicly shame organizations when they refuse to pay.

Because organizations have begun taking steps to mitigate the risks of ransomware attacks (further described below) and are increasingly able to recover their own data using backups, cybercriminals are changing their extortion techniques. They have begun moving away from ransomware attacks and appear to be focusing more on what is known as extortionware. The main difference between these attack methods is that the extortionware attacks do not involve the last step of encrypting the victim's network after exfiltrating valuable data. As noted above, the development of ransomware is typically handled by operators who charge a rental fee or sale price for the ransomware. Some groups even hire cyber actors to perform the execution of the ransomware on the victim network. Generative artificial intelligence tools may, however, reduce the costs of such activities and allow less sophisticated cyber actors to perform these activities. Additionally, to increase the chances that victims will pay a ransom, we expect that cybercriminals will begin using tactics that will result in the corruption or deletion of data on a victim's network with more frequency in 2023 and 2024. Russian APT groups have intensified their use of data-wiping malware attacks in cyberwarfare operations targeting Ukrainian networks since the military invasion and, although many of those wiper attacks have been thwarted, they may nonetheless continue and be directed against geographic areas outside of Ukraine.

A. *Mitigation of Ransomware Risks*

Ransomware is a tool used by both cyber criminals as well as APTs due to its efficacy in debilitating both public and private sector organizations. Construction companies have been a top target for ransomware attacks as well as schools and municipalities as they often lack effective cybersecurity measures. While pernicious, ransomware can be mitigated through the development and deployment of preventative and corrective cybersecurity controls. Below is a list of recommendations to mitigate the risks of being a victim of ransomware.

Implement Network Segmentation. Malware spreads quickly across information systems. By splitting the network into smaller subnetworks and isolating network traffic, organizations can decrease the surfaces vulnerable to the attack and obstruct the lateral movement of malware. In this way, a malware infection in one area of the network – a subnetwork – will not impact systems in another. It is important that organizations segment resources by their type and function, specifically any resources that are accessible via the internet. This may include placing webservers in a screened subnet (i.e., a DMZ), ensuring that user workstations and servers are on separate Virtual-LANs ("VLANs"), and ensuring that inter-VLAN traffic is routed through a next-generation firewall ("NGFW").

Use Multi-Factor Authentication ("MFA"). Ransomware is often deployed through credential abuse by a threat actor. These threat actors will compromise a user account, and then seek to exploit a privileged user account (i.e., a system administrator account) to deploy malware on the victim's network. MFA is the most effective method to block this threat vector. Companies should deploy MFA for all users to authenticate to company systems. However, if this is impractical, MFA should be required for all remote access and privileged accounts to help mitigate the risk of ransomware.

Create and Test Regular Data Backups. While ransomware actors will typically hold critical business data for ransom, companies can negate this leverage by making regular backups of company data and storing them on a secure location that is not connected to the network (i.e., a system that is not accessible by the same trust

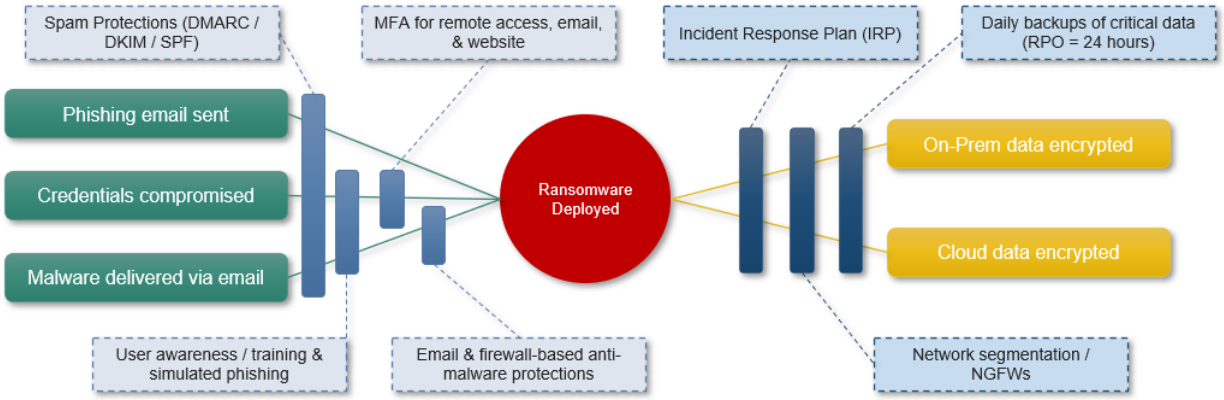
domain as the original data, ensuring that attackers cannot also encrypt the backups such as an offsite location or cloud-based backup service). Companies should determine the Recovery Point Objective ("RPO") for their data, the cadence of backups (*i.e.*, full, differential, and incremental backups as well as VPC replication and snap shots in cloud environments), and regularly test their backups to ensure sufficient fidelity.

Establish and Maintain an Incident Response Plan ("IRP"). While companies can attempt to prevent the deployment of malware, as noted above, no organization is immune to a cyberattack. It is therefore imperative that organizations develop, maintain, and test an IRP. A well-designed IRP incorporates five key elements: (1) preparation; (2) detection and analysis; (3) containment, eradication, and recovery; and (4) post-incident activity/lessons learned.[18] The first 24 hours after you discover a data breach are critical to (1) restoring your network security, (2) obtaining and preserving evidence for the cyber investigation, and (3) complying with your legal and contractual obligations. With regard to ransomware, the IRP should address organizational processes for mitigating ransomware that has been deployed, escalation requirements, and key points of contact. Government contractors should pay special attention to incident reporting requirements contained in government contracts, including obligations and timeframes for reporting cybersecurity incidents. A critical and often overlooked piece of the IRP is your internal and external communication plans to affected individuals and entities – employees, investors/shareholders, business partners, and customers. Even if your customers' information was not compromised, your business may not be able to meet its contractual or construction deadlines or your email network may not be secure or operational. Making prompt and timely disclosures may mitigate losses and potential liability. Additionally, a lack of transparency about a data breach could cause permanent and substantial reputational harm.

Adopt a Zero-Trust Architecture ("ZTA"). With the proliferation of remote work and the use of cloud infrastructure, many organizations, both in the government and private sector, are moving to ZTA. ZTA provides a more granular approach to

security leveraging many of the techniques above (*i.e.*, MFA, network segmentation, etc.). ZTA focuses on ensuring there is a check of identity (authentication) and access permissions (authorization) at every step of the digital transaction. Many technologies support ZTA, but in essence it is a departure from the traditional security approach of established trust boundaries where subjects within the boundary are "trusted" to access objects within the boundary.

Figure 1 – A Bow Tie analysis of security control mitigations for ransomware. The left side of the ransomware deployment represents preventive controls while the right side represents corrective controls.



B. *Ransom Payments May Violate U.S. Sanctions*

The decision to pay a ransom to a malicious cyber actor that has encrypted a company's network and/or stole a company's data and is threatening to sell the data on the darkweb is often a difficult dilemma involving several factors. In some instances, it is illegal to pay a ransomware group or cyber actor because they are located in a sanctioned designation, such as Iran, or the entity or person has been designated as a specially designated national ("SDN") and blocked person by the U.S. Government. The Department of Treasury's Office of Foreign Asset Controls administers and publishes this SDN list. These sanctions prohibit U.S. companies from engaging in transactions with, or providing financial services to, sanctioned countries or specially designated nationals and blocked persons. Additionally, because the standard for civil liability for violating economic sanctions is strict liability, companies face severe civil penalties even if there is no negligence, intent, or other

finding of fault. Violations of OFAC's economic sanctions programs can give rise to criminal liability if the violation was intentional and committed knowingly. These violations are prosecuted under the International Emergency Powers Act, 50 U.S.C. §§ 1701-1708 and carry a lengthy maximum term of imprisonment of 20 years.[19]

V. U.S. Government Approach to Managing Cyber Threats

A. *National Cybersecurity Strategy*

On March 3, 2023, the Biden Administration released its National Cybersecurity Strategy.[20] This 35-page strategy document describes the significant and evolving cyberthreat environment and unsurprisingly, consistent with ODNI's 2023 Annual Threat Assessment, identified the PRC as the "broadest, most active, and most persistent threat to both government and private sector networks." The strategy document also sets forth aspirational goals of building a more "resilient digital ecosystem," improving cyber defenses, addressing cybercrime using both the Department of Defense and Department of Justice, and creating minimum mandatory cybersecurity requirements and increased liability for the private sector. The implementation of these goals will take time and buy-in from the private sector. Here are three of the most important elements of this strategy for the construction industry.

First, in recognition of the billions of dollars of damages caused by ransomware and cybercrime, the strategy calls for making changes to the digital ecosystem and modernizing federal defenses. The strategy indicates that the Department of Defense as well as Department of Justice ("DOJ") will be increasing the speed, frequency, and scale of disruption campaigns against both state and non-state cyber actors. This is critical as small to mid-sized businesses are ill equipped to respond to advanced persistent threats and attacks by malicious state actors. The strategy also acknowledges that intelligence agencies need to declassify cyber threat information and share it broadly with industry and academia. The classification of information has often been an obstacle in cyberspace. Additionally, over the last two years, government officials have criticized the private sector for not sharing information about cyber incidents and the lack of reporting information has stymied efforts for law enforcement to investigate cyber actors and the government's ability to

respond to cyberattacks. Here too, the strategy document repeats the importance of reporting cyber incidents and indicates that entities in the critical infrastructure sectors will be required to report cyber incidents to the government within hours of discovery as a result of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). The CIRCIA is discussed further below.

Second, the Biden Administration wants to shift the burden from individuals and small companies to software companies, manufacturers, and third-party providers for creating cyber resiliency. Rather than adding cybersecurity to a product after it is developed or produced, cybersecurity requirements need to be built into the software or hardware from the beginning. These principles were recently highlighted by Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") in a publication entitled "Security-by-Design and –Default."[21] The Administration is calling for laws to establish greater liability for software companies and manufacturers that fail to build minimum security standards into their products. By baking-in security that would eliminate the need for companies and individuals to continuously patch critical vulnerabilities that are often exploited by cyber actors. The strategy document further mandates the establishment of mandatory cybersecurity requirements for critical infrastructure and third-party service providers, including cloud-based services. The strategy document also highlights DOJ's Civil Cyber Fraud Initiative and DOJ's intent to hold defense contractors liable for cybersecurity non-compliance.

Lastly, the strategy document indicates that the administration will explore a federal cyber insurance backstop to stabilize insurance markets against catastrophic losses. This is an extremely important issue to businesses in light of the decision by Lloyd's of London, the world's largest insurance marketplace, in August of 2022 to exclude state-backed cyber-attacks and the statement of the CEO of Europe's Zurich Insurance on December 26, 2022 that cyberattacks are becoming "uninsurable." Cyberattacks affecting supply chains have caused unprecedented losses and destructive damage to critical infrastructure. Merck spent years fighting its insurer to cover massive losses of $1.4 billion caused by Russia's NotPetya malware attack. In May of this year, the New Jersey appeals court rejected the insurers' argument that the Russia's cyberattack constituted a "hostile or warlike action by a

government," which was excluded from coverage under the policy.[22] On July 19, 2023, the New Jersey Supreme Court agreed to hear this matter so this case is not yet resolved.

B. *Legislation*

i. Executive Orders

In response to the escalation of crippling cyberattacks, including the Colonial Pipeline ransomware attack, and the government's perceived inability to respond because it lacked information from the private sector, on May 12, 2021, President Biden issued Executive Order 14028 on improving the Nation's cybersecurity. EO 14028 directed government agencies to improve cybersecurity and take measures to protect critical infrastructure, including finding ways to encourage more coordination and cyber incident reporting by the private sector. Additionally, EO 14028 required each government agency to conduct a comprehensive cyber review to determine how it could assist the government in its aim to increase cybersecurity in private and public sectors. After the signing of EO 14028, the DOJ announced its Civil Cyber-Fraud Initiative (described below), DHS formed a Cyber Safety Review Board, the Federal Trade Commission announced its intention to seek enforcement actions against organizations that fail to mitigate known cybersecurity vulnerabilities, and the Securities Exchange Commission ("SEC") proposed new cybersecurity disclosure rules substantially increasing public companies reporting obligations.

ii. Industry regulation

SEC Enforcement Actions. Over the last few years, the SEC has started scrutinizing cybersecurity procedures and controls and has brought numerous enforcement actions against public companies related to data breaches. In June 2021, the SEC sanctioned real estate title insurance company First American for failing to "have any disclosures controls and procedures related to cybersecurity" to ensure that senior officials were apprised of pertinent cybersecurity vulnerabilities, risks, and assessments in making public disclosures.[23] In August 2021, the SEC charged Pearson plc, a London-based educational publishing company, with misleading investors about a 2018 cyber intrusion.[24] Pearson agreed to pay $1 million to settle the charges it had made misleading statements

and omissions about the 2018 data breach, which involved the theft of millions of student records, and had inadequate disclosures controls and procedures. In March 2023, the SEC charged Blackbaud Inc., a South Carolina company, with making misleading disclosures about a ransomware attack and fined it $3 million.[25] The SEC found that "Blackbaud failed to disclose the full impact of a ransomware attack despite its personnel learning that its earlier public statements about the attack were erroneous."[26] This action underscores the importance of having controls and procedures in place to ensure disclosures about the scope of cyberattacks are accurate and senior management is regularly updated about the status of a cyberattack.

According to the SEC's Complaint against Blackbaud, on July 16, 2020, Blackbaud, a public company that provides donor data management software to non-profit organizations, announced on its website that it had been a victim of a ransomware attack in May 2020 and notified its customers.[27] In its announcement, the company indicated that the hackers did not access any donor bank account information or social security numbers. Within days of these statements, however, Blackbaud's technology and customer relations employees learned that these claims were wrong and that the hackers had accessed and exfiltrated its donors' bank account information and social security numbers.[28] Numerous customers had raised concerned after Blackbaud's initial disclosure and, as a result, the company conducted further investigation and determined that certain donor bank account and information had indeed been accessed and exfiltrated by the attacker in unencrypted format.

Nevertheless, on August 4, 2020, the company filed a Form 10-Q (a Form 10-Q is a quarterly report required to be filed by all public companies with the SEC), which discussed the ransomware attack but "omitted this material information about the scope of the attack, and misleadingly characterized the risk of exfiltration of such sensitive donor information as hypothetical."[29] The SEC concluded that Blackbaud's Form 10-Q filing "perpetuated the false impression, started with the company's earlier website post and customer notices, that the incident did not result in the attacker accessing highly sensitive donor data" when in fact certain company personnel knew that was false.[30] Blackbaud's senior management responsible for the company's SEC disclosures were not made aware

of these facts prior to the company filing its Form 10-Q on August 4, 2020. Nor were there controls or procedures designed to ensure that information relevant to cybersecurity incidents and risks were communicated to the company's senior management and other disclosure personnel. Blackbaud did not announce the full and true scope of the ransomware attack until the end of September 2020.[31]

These actions illustrate how aggressive the SEC has become in the area of cybersecurity. Like DOJ, the SEC has decided to make this area one of its priorities and will likely continue to bring enforcement actions against public companies for failing to implement adequate cybersecurity controls and make accurate and timely disclosures concerning material cybersecurity incidents such as cyberintrusions and data breaches.

As of the date of this paper, on June 24, 2023, SolarWinds reported that the SEC has issued Wells Notices against its former and current executives, including its Chief Information Security Officer and Chief Financial Officer.[32] The SEC issues Wells Notices to a person or corporate entity when it intends to institute an action and bring charges against them.[33] As a result, victims of cyberattacks therefore need to understand that their actions could provide the basis for both civil and criminal enforcement actions.

With constantly evolving cyberthreats and persistent foreign state backed hackers, it is difficult to thwart every cyber actor. Enforcement actions (like those currently being considered by the SEC with regard to SolarWinds) could prove detrimental to the government's initiatives designed to promote private-public partnerships and have a chilling effect on the private sector's future cooperation and cyber incident disclosure. The SolarWinds cyberattack, orchestrated by Russian government hackers, was "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector,"[34] which even took U.S. government officials months to detect.

SEC Cybersecurity Rules. On July 26, 2023, the SEC adopted new controversial cybersecurity incident reporting rules for public companies subject to the reporting requirements of the Securities Exchange Act of 1934. These new rules went into effect in September 2023. In a 3-2 vote, the SEC approved disclosure requirements that will require public companies to publicly report any cybersecurity incident that they determine to be

"material" within four business days of making that determination on an 8-K form with the SEC.[35] This materiality determination must further be made "without unreasonable delay."[36] The new SEC rules also impose periodic disclosure requirements about cybersecurity risk management, strategy, and governance.

On the 8-K form, companies will need to describe the "material aspects of the nature, scope, and timing of the [cybersecurity] incident, as well as the material impact or reasonably material impact of the incident" on the reporting company "including its financial condition and results of operations."[37] Additionally, in its final rule, the SEC instructed companies to consider both qualitative as well as quantitative factors in assessing "the material impact of an incident" including "harm to a company's reputation, customer or vendor relationships, or competitiveness" and "the possibility of litigation or regulatory investigations or actions … by state and Federal governmental authorities and non-U.S. authorities."[38]

As a result of the voluminous comments it received, the SEC did make some changes to its proposed rules announced in March 2022,[39] which eliminated the need to detail technical information such as how the cyber incident occurred (i.e., how the hackers gained access to the networks).

Many commentators, including cybersecurity firm Rapid7, Inc., explained that mandating that companies publicly disclose this type of technical information could result in further harm to the reporting company and "copycat attacks on other companies" by other malicious actors seeking to exploit the same vulnerability.[40] As Rapid7 noted in its August 2022 comments, "fewer than 100 organizations were actually exploited through the Solarwinds supply chain attack, but up to 18,000 organizations were at risk."[41]

Despite the changes the SEC made to its final rules, these rules will nevertheless be difficult for many companies to comply with by the December 18, 2023 deadline for reporting cybersecurity incidents. This deadline was extended for additional 180 days for small companies. Cyberattacks are not typically contained, investigated, remediated in a matter of days. Yet, such disclosures will be required to be publicly filed and executives will be held accountable for any false or misleading statements made about cybersecurity incidents. Disclosures to the SEC will likely take precedent over compliance with state

data breach laws as the vast majority of states require that breach notifications be made between 30 to 60 days after determining a data breach occurred.

Most significantly, within four days of discovering a likely material cybersecurity incident such as a ransomware attack, organizations do not know the true scope of the incident and likely do not know (1) how their network was accessed (2) whether any backdoors still remain on their network, (3) how long cyber actors have been hiding on their network and accessing files, and (4) what data/files were compromised. Very often, the initial assessments and findings concerning a cybersecurity incident are erroneous. Breach counsel therefore advise clients to wait until the forensic investigation is completed before making any disclosures about its scope and the data that was, or reasonably likely, compromised. Furthermore, as the National Association of Corporate Directors stated the four-day incident reporting deadline "may not allow companies the time to put in place adequate patches and protections before being forced to make it known that they have been compromised digitally." This could lead to attack escalation. In addition, during this short four-day reporting time frame, organizations may still be trying to determine attribution or could be engaged in negotiations with the cyber actors to gain necessary intelligence.

Further, the SEC is only allowing a limited law enforcement exception to this reporting requirement. This exception needs to be approved by the U.S. Attorney General within the four-day discovery deadline and, for that exception to apply, the Attorney General must determine "that the disclosure poses a substantial risk to national security or public safety." While it appears that the SEC has established an interagency communication process to allow for the Attorney General's determination to be communicated" to the SEC in a timely manner, it is unlikely that this exception will apply to most cyberattacks, including the increasing number of ransomware attacks.

These new SEC disclosure requirements will undoubtedly create significantly more liability risk and compliance requirements for companies, many of which will also be subject to the new 72-hour incident reporting rules currently being developed by the Cybersecurity and Infrastructure Security Agency for organizations involved in critical

infrastructure. In adopting its new rules, the SEC dismissed potential conflicts with the CIRCIA rules (described below) and at this time, it is unclear how any conflict between these two sets of rules may be resolved. What is clear, however, is the importance of having reasonable cybersecurity controls and effective cybersecurity risk management and oversight processes.

CIRCIA. Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), companies falling within 16 broadly defined critical infrastructure sectors will be required to report material cybersecurity events to CISA within 72 hours and report any ransomware payment within 24 hours. These 16 critical infrastructure sectors are:

(1) Chemical
(2) Commercial Facilities
(3) Communications
(4) Critical Manufacturing
(5) Dams
(6) Defense Industrial Base
(7) Emergency Services
(8) Energy
(9) Financial Services
(10) Food and Agriculture
(11) Government Facilities
(12) Healthcare and Public Health
(13) Information Technology
(14) Nuclear Reactors, Materials, and Waste
(15) Transportation Systems
(16) Water and Wastewater Systems

CISA is currently working on drafting the regulations applicable to these requirements, including terms like "material cybersecurity incident" and what types of information will be required to report to the government.[42] Within 72 hours of discovery of

a cybersecurity incident, organizations often have very little information and typically do not know the true scope of the compromise or how much data may have been accessed or exfiltrated. Extensive reporting requirements will therefore be difficult, if not impossible, for many organizations until a thorough cybersecurity forensic investigation has been completed.

Federal Trade Commission. Beginning in 2022, the Federal Trade Commission has signaled through its statements and enforcement actions that one of its priorities is cybersecurity compliance, specifically how companies protect consumer and employee personal data in an increasingly digital economy. In September 2022, it held a virtual public forum on the agency's release of an Advance Notice of Proposed Rulemaking to regulate the protection of consumer's privacy and data security.[43]

Recently, the FTC has been increasing its use of enforcement by regulation for its stated purpose of protecting consumers. Three primary areas have been a focus for the FTC: (1) violating children's privacy laws; (2) sharing information about consumer's online activity with third parties; and (3) lax cybersecurity. Epic Games paid $275 million to settle FTC allegations that it violated the Children's Online Privacy Protection Act ("COPPA") and the FTC fined Twitter $150 million for using account security data for targeted advertising in violation of a 2011 consent decree.[44] In May 2023, Amazon agreed to pay more than $30 million to settle charges made concerning Ring and Alexa.[45] The FTC charged Ring, a home security camera company owned by Amazon, with compromising its customer's privacy by allowing employees and contractors to access and watch consumers' private surveillance video recordings in violation of consumer privacy. According to the FTC complaint, Ring had deceived customers about the security and privacy of its data by failing to restrict its employees or contractors from accessing customer data. The FTC pointed to egregious examples of how Ring violated its customers' privacy, including one employee who had viewed thousands of Ring video surveillance recordings of female users in their bathrooms and bedrooms. FTC also charged Ring with failing to implement basic privacy and security protections, which enabled hackers to take control of consumers' accounts, cameras, and video data. Amazon agreed to pay $25 million to settle FTC's charges that Amazon disregarded deletion requests from parents made under the COPPA and kept sensitive

voice and geolocation data relating to children for years and used it to improve its Alexa algorithm. The FTC's complaint alleged that this practice put volumes of data relating to children under the age of 13 at risk for harm from unnecessary access.

C. Increased Enforcement Landscape

On October 6, 2021, Deputy Attorney General ("DAG") Lisa Monaco announced DOJ's Cyber-Fraud Initiative to "combat new and emerging cyber threats to the security of sensitive information and critical systems."[46] This Initiative was the direct result of DOJ's ongoing comprehensive cyber review, launched as a result of EO 14028 and the government's perceived inability to respond to numerous cyberattacks against critical infrastructure (*i.e.,* SolarWinds, Colonial Pipeline, Microsoft Exchange) because it lacked information from the private sector. DAG Monaco made clear that the Civil Cyber-Fraud Initiative was designed to change behaviors of the private sector because "for too long companies have chosen silence rather than reporting breaches." Accordingly, DAG Monaco indicated that DOJ intends to use the False Claim Act ("FCA") to hold government contractors accountable for putting U.S. information and systems at risk by knowingly: (1) providing deficient cybersecurity products or services; (2) misrepresenting cybersecurity practices or protocols; or (3) failing to monitor and report cybersecurity incidents and breaches. Significantly, this initiative coincided with DOJ's repeated admonitions to businesses that it intends to increase investigations and prosecutions of corporate crime. Attorney General Garland has stated that DOJ's primary goal was to obtain individual convictions rather than just accepting big dollar dispositions.

Enacted in the 1860s in response to fraud against the Union Army, the FCA, 31 U.S.C. §§ 3729-3733, has become DOJ's primary civil enforcement tool. The FCA is extremely broad and imposes liability on anyone who "knowingly presents, or causes to be presented, a false or fraudulent clam for payment or approval" or "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim." 31 U.S.C. § 3729(a)(1). The FCA does not require specific intent to defraud to establish a violation. Knowledge of a false claim can be proven if a person has

actual knowledge that a claim is false, was deliberately ignorant of the truth or falsity of a claim, or recklessly disregarded the truth or falsity of a claim. *See id.* at 3729(b)(1).

On June 1, 2023, the U.S. Supreme Court ruled in a unanimous consolidated decision, *United States ex rel. Schutte v. SuperValu Inc. and United States ex rel. Proctor v. Safeway, Inc.*,[47] that the "FCA scienter element refers to [a] respondents' knowledge and subjective beliefs – not to what an objectively reasonable person may have known or believed." Thus, the only relevant inquiry is "what the defendant thought when submitting the false claim – not what the defendant may have thought after submitting it" or a *post hoc* interpretation.[48] Consequently, a defendant may be liable under the FCA if it either (i) "actually knew" that its conduct was unlawful; (ii) was "aware of a substantial risk" of unlawfulness "and intentionally avoided learning whether" its conduct was lawful; or (iii) was "aware of such a substantial and unjustifiable risk but submitted the claims anyway."[49]

The FCA permits the government to recover three times its losses, plus a civil penalty of $13,508-27,018 for each claim. Indeed, the government has recovered over $70 billion in settlements and judgements under the FCA since 1986 and in 2022, collected over $2.2 billion in FCA recoveries.

What is unique about the FCA is that it contains a whistleblower provision, creating a financial incentive for company insiders/whistleblowers to uncover and report fraud. If the whistleblower's disclosure results in the recovery of funds by the United States, they will be entitled to 15-30% of the funds recovered.

i. First Settlement under Civil Cyber-Fraud Initiative Announced in March 2022 – Comprehensive Health Services LLC

On March 8, 2022, the DOJ announced its first settlement of a cyber fraud case since launching the Civil Cyber-Fraud Initiative. Under the settlement agreement, Comprehensive Health Services LLC ("CHS"), a provider of global medical services, paid $930,000 to resolve allegations that it violated the FCA by failing to maintain its patients' medical records on a secure network and taking adequate cybersecurity steps to store this information. CHS had contracted to provide medical support services at government-run facilities in Iraq and Afghanistan, but, according to the FCA complaint, ignored the privacy

concerns of staff about the storage of protected health information. The whistleblowers therefore commenced this action. In its press release announcing this settlement, DOJ indicated that it would aggressively pursue government contractors that fail to follow cybersecurity standards.[50]

ii. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*

On April 26, 2022, less than 24 hours after the jury had been impaneled and before any witnesses had testified in the first cyber-related fraud *qui tam* trial, *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc. ("Aerojet"),* Aerojet agreed to pay more than $9 million to settle the case. The whistleblower (also known as a *qui tam* relator), Aerojet's former senior director of cybersecurity, had brought a FCA suit in the U.S. District Court for the Eastern District of California, on behalf of the government, alleging that Aerojet had lied to the government about its compliance with applicable cybersecurity requirements to obtain contracts with DOD and NASA from 2013 to 2015 and sought damages in excess of $19 billion – three times the sum of every invoice paid under the fraudulently obtained contracts. The *Aerojet* trial was the first-of-its-kind cybersecurity non-compliance FCA case to get to trial.

After being fired by Aerojet, the whistleblower brought a wrongful termination and FCA case against Aerojet in 2015. The whistleblower alleged that Aerojet knowingly misrepresented its compliance with applicable cybersecurity requirements (including DFARS Section 7012) and thereby fraudulently obtained contracts with DOD and NASA. The whistleblower contended that the cybersecurity requirements were material and sought damages for every claim the government paid under contracts it entered with Aerojet from 2013 to 2015. In 2018, DOJ declined to intervene in this action. Yet, two weeks after the Cyber-Fraud initiative was announced, in October 2021, DOJ filed a Statement of Interest in support of the relator's arguments opposing summary judgment. With DOJ's assistance, the whistleblower defeated Aerojet's summary judgment motion.

The U.S. District Court rejected Aerojet's arguments that the contracts' cybersecurity control provisions were not material and the government did not suffer any damages because it had delivered functional rocket engines.[51] This argument ignored the fact that

the government also contracted with Aerojet to store the government's technical data concerning its missile systems on a secure network. Accordingly, the issue of materiality and damages would be resolved by a jury.[52] This risk proved too much for Aerojet, especially after hearing the relator's opening statement detail critical deficiencies in Aerojet's network security that made it vulnerable to cyber-attacks during the relevant time period. Aerojet agreed to pay $9 million to settle the FCA claim and an additional undisclosed amount for attorney's fees. This quick settlement signals how precarious the situation has become for companies that do not comply with contractual cybersecurity requirements and fail to adequately safeguard government information.

During pre-trial litigation, Aerojet unsuccessfully argued, first in a motion to dismiss, and later in a summary judgment motion, that the applicable cybersecurity requirements were not material because it disclosed to the government that it was not fully compliant with them. The Court disagreed and denied both motions. In its summary judgment decision, the Court concluded that materiality was an issue for the jury and there was a triable issue of fact regarding the "sufficiency" of Aerojet's disclosures.[53] The Court further found that the whistleblower presented evidence demonstrating that Aerojet had concealed the true breadth of its noncompliance from the government; it did not share with the government information about data breaches or the results of external audits detailing numerous deficiencies.[54]

The whistleblower also defeated Aerojet's summary judgment motion on damages.[55] Aerojet argued that there was "no evidence that the government suffered actual damages" because it had supplied defect free, functional rocket engines as required under the contracts. The Court found that the government contracts, however, also required Aerojet to store the government's technical data on a secure network that met applicable cybersecurity requirements.

Shortly after the Court issued its summary judgment decision, the trial began. In its opening statement, the whistleblower juxtaposed Aerojet's sensitive missile defense work for DOD with its deficient cybersecurity practices, undisclosed data breaches, and cybersecurity non-compliance. On the second day of trial, Aerojet agreed to settle the case for $9 million. The whistleblower was awarded $2.61 million, which represented 29% of this

recovery. On July 8, 2022, DOJ's press release announcing the recovery highlighted the critical role whistleblowers like Markus "with insider information and technical expertise" can serve "in identifying knowing cybersecurity failures and misconduct."[56] Less than two weeks later, DAG Monaco referenced the Aerojet settlement in a speech announcing the disruption of the activities of a North Korean state-sponsored group deploying ransomware known as "Maui." In this speech, she encouraged the private sector to report cyberattacks and signaled the importance of cybersecurity compliance to the security of our cyber ecosystem: "Holding contractors accountable for their cybersecurity promises will enhance resiliency against cyber intrusions across the government, the public sector, and key industries."[57]

iii. Jellybean Communications Settlement for Cybersecurity Failures

On March 14, 2023, DOJ announced the third settlement under the Civil Cyber-Fraud Initiative. Jelly Bean Communications Design LLC ("Jelly Bean") and its manager agreed to pay $293,771 to resolve FCA allegations that it failed to properly secure personal information on a federally funded Florida children's health insurance website it created, hosted, and maintained. Parents of children aged 5 to 17 used this website to apply for children's health insurance.[58]

Despite its contractual representations and obligations to provide a fully-functional hosting environment that complied with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Jelly bean did not provide a secure hosting for personal information and failed to properly maintain, patch, and update its software systems and related websites, leaving the site and data Jelly Bean collected from applicants vulnerable to cyberattacks. And that is exactly what happened. In December 2020, the website was hacked and over 500,000 health insurance applications were compromised. These insurance applications contained dates of birth, social security numbers, financial information, and insurance information. The investigation further revealed that Jelly Bean had not updated or patched some of the software used on its website since 2013, the same year it had entered the contract with Florida.

iv. Criminal Liability – Prosecution and Conviction of Joseph Sullivan, Uber's Chief Security Officer

In October 2022, a jury convicted Joseph Sullivan ("Sullivan"), Uber's former Chief Security, of obstructing justice by failing to report a new data breach of Uber while it was being investigated by the FTC for a prior one. This case marks the first time a corporate officer was held criminally liable for actions related to the handling of a data breach, but it is unlikely to be the last.

Sullivan was a former federal cybercrime prosecutor and cybersecurity expert. Before joining Uber, Sullivan was the Chief Security Officer at Facebook and had worked in security roles at both eBay and Paypal. In May 2015, one month after Sullivan began working at Uber, the FTC served Uber with notice that it was investigating its data security program and practices related to a data breach that occurred in 2014. Sullivan played an integral role in Uber's response to the FTC investigation. Most importantly, in November 2016, Sullivan told the FTC during sworn testimony that Uber had improved its cybersecurity and fixed the problems that led to the data breach in 2014. 10 days after Sullivan's deposition, however, Uber suffered another data breach.

During Uber's 2016 data breach, hackers downloaded voluminous data that Uber had stored on Amazon Web Services and sent a ransom note, which made clear that they expected a six-figure payout. According to the evidence presented at trial, Sullivan sought to use a bug bounty program to pay the hackers even though the program was not designed for this purpose and had a maximum payout of $10,000. Bug bounty programs are typically provided to white hat hackers who find a vulnerability and notify the company about the vulnerability before it can be exploited for nefarious purposes. Nonetheless, Sullivan arranged for the hackers to be paid $100,000 through Uber's private bug bounty program in bitcoin in exchange for them signing a non-disclosure agreement which falsely stated:

> You promise that you did not take or store any data during or through your research and that you have delivered to us or forensically destroyed all information about and/or analyses of the vulnerabilities.

Additionally, the prosecutors claimed that Sullivan provided a misleading summary of the 2016 data breach to Uber's new Chief Executive Officer making it appear as though the hackers had accessed some rider and driver data, but no data was actually taken. Indeed, the hackers accessed and downloaded the driver's license numbers of

approximately 600,000 Uber drivers in addition to the names, emails, and mobile phone numbers of approximately 57 million Uber users. At a minimum, in 2016 when this data breach occurred, California law required Uber to notify affected California residents if their unencrypted personal information was acquired by an unauthorized person. Because of the actions of Sullivan and others at Uber, the 2016 hack was kept secret for more than a year until the new CEO's legal team disclosed it to DOJ.[59]

In July 2022, Uber entered into a Non-Prosecution Agreement with DOJ in which it admitted and accepted responsibility for the acts of its officers, directors, employees, and agents in concealing the 2016 data breach from FTC and agreed to pay $148 million. As part of settlement, Uber agreed to implement a corporate integrity program, specific and robust data security safeguards, comprehensive information security program, and a comprehensive incident response and data breach notification plans along with biennial assessments of Uber's information security program by an independent third party for a period of 10 years.

After a three-week trial that included the testimony of one of the two hackers, the jury convicted Sullivan of obstructing justice and misprision of a felony. DOJ made clear in announcing the verdict that it "will not tolerate concealment of important information from the public by corporate executives more interested in protecting their reputation and that of their employers than in protecting users. Where such conduct violates the federal law, it will be prosecuted."[60] DOJ sought a sentence of 15 months' imprisonment for Sullivan's crimes. The Court, however, declined to impose a sentence of imprisonment citing to the fact that this was an "unprecedented" case. Instead, he sentenced Sullivan to a three-year term of probation. The judge, however, made clear that if similar conduct occurs in the future, individuals will not be shown leniency but rather "should expect to spend time in custody."[61]

Although this case on its facts is atypical in that Uber suffered a second cyberattack while being investigated by a federal agency for a prior data breach, it should serve as a warning that DOJ will be seeking jail time against corporate insiders who choose to cover up embarrassing cybersecurity mistakes and lie to federal officials. There may be a large pool of potential DOJ targets based upon the Bitdefender 2023 Cybersecurity Assessment.

That report found that "71%" of cybersecurity teams in the United States "have been told to keep a security breach confidential when it should have been reported." The decision to conceal data breaches and not make the mandated disclosures may result in significant criminal and civil liability, especially if your employees decide to become whistleblowers. In addition to governmental investigations, organizations that fail to comply with state data breach laws could also face class-action lawsuits for engaging in unfair and deceptive trade practices.

VI. The Controlled Unclassified Information Program and Cybersecurity Requirements for Non-Federal Entities

The U.S. Government's approach to enhancing the nation's cybersecurity has included actions from both the Legislative and Executive Branches of government. This whole-of-government approach has led to multiple laws and executive orders that apply to U.S. federal agencies, government contractors, critical infrastructure entities, and private industry. Of particular significance, federal agencies have enacted regulations requiring cybersecurity protections be included in federal acquisition contracts.

In the aftermath of 9/11 attacks, an independent, bipartisan commission was created to identify the causes of the failure in predicting and preventing the worst terrorist attack on American soil. The 9/11 Commission Report[62] identified several causes of this failure, one was a failure to share sensitive, but unclassified information, due to balkanized, non-uniform agency safeguarding requirements. A key recommendation from the Commission was for the President to lead a policy effort to enhance information sharing among federal agencies "guided by a set of practical policy guidelines that simultaneously empower and constrain officials, telling them clearly what is and is not permitted."[63]

In 2010, President Obama issued Executive Order 13556, which established the Executive Branch's Controlled Unclassified Information ("CUI") program. This CUI program was designed to establish "an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies…" The Order designates the National Archives

and Records Administration ("NARA") as the Executive Agent charged with implementing the Executive Branch CUI program. NARA was tasked with creating, through inter-agency discussions, a CUI Registry which defines the various types of federal agency CUI and references dissemination authorities for each (*i.e.*, federal statutes or regulations which grant the agency authority to place dissemination controls upon the category of CUI). To support this effort, NARA began rulemaking to promulgate a rule, which would provide uniform guidance to all federal agencies on how they shall protect CUI in their possession as well as CUI that they share with partners and government contractors.

In 2016, the CUI Final Rule was published, establishing the Executive Branch's requirements for the handling and dissemination of CUI. In addition to delineating how federal agencies must designate, handle, and decontrol CUI, it also addresses how agencies may effectuate protections of CUI in non-federal entities.[64]

VII. Test Case – CUI and the Department of Defense

Defense contractors are required to comply with cybersecurity standards set forth in the "Safeguarding Covered Defense Information and Cyber Incident Reporting" clause at Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012 ("Section 7012" or "Clause 7012"). When the CUI Final Rule was issued, the DOD had already begun the rulemaking process to update the DFARS 252.204-7012 clause, which would bifurcate cybersecurity requirements between two data types: (i) Federal Contract Information ("FCI"); and (ii) various data types designated by DOD distribution statements that would ultimately become a category of CUI – Controlled Technical Information ("CTI"). In 2016, DFARS Section 7012 was issued as a final rule, implementing NIST SP 800-171 requirements for covered contractors who would receive CUI. The lower tier of FCI cybersecurity was finalized as a FAR requirement – 52.204-7012 *Basic Safeguarding of Covered Contractor Information Systems* – requiring covered contractors to implement 15 security requirements, which equate to the 17 Basic Requirements of NIST SP 800-171.

Section 7012 ultimately established NIST SP 800-171 as the minimum for implementing "adequate security" on covered contractor information systems. *See* 252.204-7012(b). This clause contained requirements relating to cyber incident reporting,

DOD forensic access to compromised systems, and forensic evidence retention. Of particular importance to DOJ's Civil Cyber-Fraud Initiative, Section 7012 requires that defense contractors "rapidly report" cyber incidents to DOD within 72 hours of discovery. Finally, the 7012 clause at 252.204-7012(m) required that any contractor that would be sharing DOD CUI with a subcontractor was required to flow down the entirety of the clause in any subcontract. This flow-down requirement to nonfederal entities who potentially had no privity of contract with any federal agency renders agency enforcement (i.e., False Claims Act litigation) ambiguous and unpredictable.

VIII. DFARS Update and Attempts at Verification

While the DFARS -7012 and FAR 52.204-21 clauses were in effect, multiple intra- and interagency reports confirmed that critical defense data continued to leak from the Defense Industrial Base ("DIB") to strategic adversarial nations. China had produced an eerily similar replica of U.S. Fifth generation fighter aircraft, produced through the theft of DIB intellectual property and U.S. defense technical data. It was clear to the DOD and the federal government that merely requiring the implementation of a cybersecurity standard was not sufficient, and that through either ignorance or fraud, the DIB was unable or unwilling to shore up CUI data held or created on behalf of the DOD.

2020 saw the finalization of three interim final rules, which produced new DFARS cybersecurity-focused contract clauses and the mandatory use of a companion guide to SP 800-171, the SP 800-171A *Assessing Security Requirements for Controlled Unclassified Information*. The latter remains a point of confusion for many contractors leading to potential insufficiency of program implementation and veracity of representations of cybersecurity compliance to DOD officials.

DFARS 252.204-7019 – This clause requires that covered contractors assess the implementation of NIST SP 800-171 on their own systems using the NIST SP 800-171A and DOD Assessment Methodology ("DODAM") which would be used to produce a summary score submitted to the DODs Supplier Performance Risk System ("SPRS"). This assessment was called a "Basic Assessment." This Basic Assessment would allow the DOD to have visibility into the implementation of NIST SP 800-171

in the DIB at large, but also make more informed risk decisions when selecting contractors. This requirement, like the Section 7012 clause, contained a flow down requirement, meaning that both prime and subcontractors would be required to conduct such assessments. Notably, this clause created a requirement for contractors to make a material representation of their cybersecurity compliance to the DOD, which laid the groundwork for FCA litigation as internal DOD guidance requires contract officers to use the SPRS system during the contractor selection process.

DFARS 252.204-7020 – This clause established the categories of Medium and High Assessments. Both assessments would be carried out by the Defense Contracts Management Agency ("DCMA") Defense Industrial Base Cybersecurity Assessment Center ("DIBCAC") with a Medium Assessment being comprised of a review of the covered contactor's System Security Plan ("SSP") and supporting governance documentation, and a High Assessment being compromised of a detailed audit of the covered contactor system, including high fidelity verification of some or all of the 110 security requirements of NIST SP 800-171. This clause provided the first opportunity for the DOD to directly validate the representations made by contractors to the DOD under the -7012 and -7019 clauses.

DFARS 252.204-7021 – Understanding that it could not rely on contractor representations of compliance or scale the efforts of DIBCAC to audit NIST SP 800-171 implementation throughout the DIB, the DOD, in collaboration with industry stakeholders, developed the Cybersecurity Maturity Model Certification ("CMMC"). The CMMC was an independent third-party verification mechanism that would provide a market solution to assess and certify the tens of thousands of DIB companies with a NIST SP 800-171 contract requirement. This contract clause, when finalized would represent the end of independent verification of contractor information systems and be similar to the current Federal Risk and Authorization Management Program ("FedRAMP").[65]

The CMMC envisioned the creation of an ecosystem of third-party CMMC assessors and advisors, overseen by the CMMC Accreditation Body ("AB"), that would review the

standards for training, assessment, and accreditation relating to the CMMC. The CMMC AB, initiated with much fanfare, would, with the imprimatur of the DOD, oversee the training and accreditation of several Certified Third-Party Assessment Organizations ("C3PAOs").

IX. CMMC and the Future of Defense Industrial Base Cybersecurity

The initial CMMC rule proposed the implementation of a maturity model, which was developed as a joint venture between the DOD, Johns Hopkins University, and Carnegie Mellon University. The initial framework was a five-level maturity model which required covered contractors to achieve certification to Maturity Level 3 to handle CUI in performance of a DOD contract containing DFARS 252.204-7012. Maturity Level 1 would correspond to the 15 security requirements of FAR 52.204-21 (the 17 Basic Requirements of NIST SP 800-171) and would be required for participation on any defense contract that would by default include FCI.

Maturity Level 3 contained the 110 security requirements of NIST SP 800-171, the 320 assessment objectives of NIST SP 800-171A, and an additional 20 controls known colloquially as the "Delta Twenty." Additionally, Maturity Level 3 would implement requirements for organizations to develop both policies and procedures covering each of the 14 families of security requirements in NIST SP 800-171 as well as the CMMC-specific families of Asset Management, Recovery, and Situational Awareness. These "Process" requirements identified a major misalignment of understanding between the federal government and covered contractors. In order to reduce the burden of NIST SP 800-171 requirements for nonfederal entities, NIST specifically removed SP 800-53 Moderate Baseline controls that: (i) did not relate exclusively to the confidentiality of CUI ("NCO"); (ii) were uniquely federal requirements ("FED"); and (iii) were expected to be satisfied by nonfederal organizations ("NFO"). Among these NFO controls were requirements to implement policies and procedures that in its tailoring NIST assumed organizations would create without specification. The reality was that the DIB, generally, had not implemented these administrative and procedural controls, and the inclusion of them as explicit requirements in the CMMC represented an enormous material increase in compliance

burden to the DIB. It was also unclear as to how DOD intended to implemented Maturity Levels 2, 4, and 5.

The CMMC thus formed, not only a verification mechanism for NIST SP 800-171, but a material increase in requirements for covered contractors. 32 CFR § 2002 afforded agencies the ability to require protections for their categories of CUI above and beyond that of NIST SP 800-171, and prompted an uproar from government contractors. The public comment period was characterized by voluminous comments from industry, with the majority of these comments focused on the cost and burden implications of the implementation of the CMMC.

X. CMMC 2.0 and the Return to NIST SP 800-171

In November 2021, due to the amount of industry feedback, the DOD withdrew the CMMC rule and initial CMMC model (now referred to as CMMC 1.0) and issued the CMMC 2.0 framework, which saw a major reduction in defined requirements (including the "Process" requirements) and a move from 5 maturity levels to 3. Maturity Level 1 would still include the 17 FCI security requirements, Maturity Level 2 would be limited to the 110 security requirements of NIST SP 800-171 and 320 assessment objectives of NIST SP 800-171A, and Maturity Level 3 would be aligned to the now published NIST SP 800-172 *Enhanced Security Requirements for Protecting Controlled Unclassified Information.*[66] The proposed model would require self-attestation to Maturity Level 1 for FCI-only contractors, triennial C3PAO audits for Maturity Level 2 for CUI contractors, and triennial DOD audits for Maturity Level 3 which, as of yet, has no defined applicability.

CMMC 2.0 would maintain an ecosystem of third-party providers, with oversight from the renamed Cyber AB and some additional program changes which allowed for self-attestation from certain DOD CUI contractors and the potential for the DOD to provide CMMC waivers to entire programs. This change evidenced a DOD realization that the current state of DIB cybersecurity and the desired end state of CMMC 1.0 were so far apart that the only practical solution was to limit program requirements to the already existing ground

floor of NIST SP 800-171 with the DOD-afforded waiver capabilities to keep critical programs functioning in the event covered contractors could not achieve CMMC 2.0 certification.

XII. DOD is the Canary in the Coal Mine

Defense contractors have long been subject to regulated data requirements such as the ITAR and EAR, with the DOD issuing its first guidance on technical data release restrictions in 1984.[67] The DOD has also required cybersecurity controls as a discrete contract clause for over 10 years meaning that the DIB is at least familiar with cybersecurity compliance requirements.

While the DOD has been quick to address CUI security requirements in its supply chain, it is merely a bellwether for the rest of the Executive Branch agencies. 32 CFR § 2002 applies to all Executive Branch agencies, and these agencies, both individually and collectively, are moving to implement CUI security requirements both internally and with nonfederal entities via commercial contract clauses or through grants and partner agreements.

Perhaps most impactfully, the FAR clause 2017-16 (Controlled Unclassified Information), while not yet a final rule, would require federal agencies to ensure CUI protection requirements are included in federal agency acquisition contracts. Without knowing the contents of the rule, we can safely assume that it will implement requirements at least commensurate with the 32 CFR § 2002 regulation (*i.e.*, NIST SP 800-171).

On June 21, 2023, the Department of Homeland Security ("DHS") CUI final rule was published in the Federal Register. This rule will implement information security requirements in DHS contracts via the Homeland Security Acquisition Regulation ("HSAR") clauses 3052.204-71, -72, and -73. This rule includes several critical cybersecurity requirements:

- That DHS contractors provide adequate security for CUI in their possession sufficient to prevent unauthorized access or disclosure. These protections must be commensurate with DHS policies and procedures at the time of contract award. Critically, DHS has not defined a specific protection standard (i.e., NIST SP 800-171)

instead stating in response to public comment that it would defer the definition of such standards to the upcoming final FAR CUI rule.

- That DHS contractors report known or suspected cybersecurity incidents involving Personally Identifiable Information ("PII") or Sensitive Personally Identifiable Information ("SPII") to DHS within one hour of discovery and that covered contractors report any other cybersecurity incidents to DHS within eight hours.
- That DHS contractors return to DHS or sanitize any CUI according to specific contract requirements and according to NIST SP 800-88 *Guidelines for Media Sanitization*.
- That DHS contractors operating an information system on behalf of DHS which collects, processes, or stores CUI must obtain an Authority to Operate ("ATO") from the agency. This ATO process is similar to the current Federal Risk and Authorization Management Program ("FedRAMP") but includes additional DHS-specific requirements above and beyond the implementation of NIST SP 800-53 controls commensurate with the system's impact baseline (i.e., moderate baseline for CUI).

XIII. New FAR Proposed Rules Would Drastically Increase Government Contractors' Obligations and Liability Risks Under the FCA

On October 3, 2023, the FAR Council issued two extraordinarily broad proposed rules for the stated purpose of fulfilling the goals set forth in E.O. 14028, which would apply to all government contractors -- even those that only supply commercially available off-the-shelf ("COTS") products. The proposed rules relate to Cyber Threat and Incident Reporting and Information Sharing (FAR Case 2021-017) and Standardizing Cybersecurity Requirements for Unclassified Federal Information Sharing (FAR Case 2021-019). These rules would drastically increase the costs of doing business with the government, obligations of government contractors, and the liability risks under the FCA. Indeed, both rules state that compliance with the new requirements is "***material*** to eligibility and payment under Government contracts." This is clearly a reference to the materiality element of the FCA. Further, contractors would be required to certify annually and in any new contract proposals compliance with these new cybersecurity obligations creating significant FCA liability risk as well as the potential for criminal liability for making false

statements to the government. The comment period for both rules is currently open and is schedule to close on December 4, 2023. Below is a brief summary of the key provisions of both of these proposed rules.

Cyber Threat and Incident Reporting and Information Sharing (FAR Case 2021-017): This rule proposes a new FAR clause, FAR 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology. Under this new provision, which would be applicable to all government contractors and their subcontractors (through required flow-down clauses), contractors would be required to "immediately and thoroughly investigate all indicators that a security incident may have occurred" and submit information to CISA using its incident reporting portal *within eight hours* of discovery. The rule broadly defines a "security incident" as the "actual *or potential* occurrence of the following:"

- any event or series of events, which pose(s) actual or imminent jeopardy, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;
- any malicious computer software discovered on an information system; or
- transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

After reporting the incident to CISA within eight hours, contractors would be required to update this information e*very 72 hours thereafter* until all eradication or remediation activities have been completed. Additionally, the proposed FAR cause would impose several requirements on contractors, including the preservation of data relating to the security incident for 18 months, disclosure of any malicious code samples or artifacts to CISA within eight hours of discovery, and providing CISA, FBI, and the relevant contracting agency full cooperation and access to the contractor's applicable information systems and personnel related to any reported security incident.

This proposed reporting requirement would be by far the most stringent and burdensome federal cybersecurity incident regulation with the shortest disclosure

deadline. It would require companies in a matter of eight hours to quickly assess and make determinations about complicated issues likely without having the benefit input of forensic experts or senior members of their management when they may also be in the early hours of their incident response and containment activities. Additionally, these reporting requirements will inevitably need to be made during weekends and holidays when cyber threat actors like to strike further complicating compliance. In comparison, as highlighted above, DFARS Section 7012 requires reporting of cyber incidents within 72 hours.

This rule also contains a requirement for government contractors to maintain and provide a Software Bill of Materials for any software used in the performance of the contract, which was not expected and has raised numerous concerns for government contractors of all sizes. This requirement appears impractical at this time for many companies. The SBOM would have to be updated when any piece of computer software was updated.

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems (FAR Case 2021-019): This rule proposes two new FAR clauses, FAR 52.239-XX and 52.239-YY Standardizing Cybersecurity requirements for Unclassified Federal Information Systems. These new provisions would be applicable to prime contractors as well as subcontractors that either operate Federal Information Systems ("FISs") in non-cloud computing services (FAR 52.239-YY) or operating cloud computing services (FAR 52.239-XX) on behalf of a federal agency.

FAR Clause 52.239-YY would require federal agencies to categorize FISs as either "Low," "Moderate," or "High Impact" using FIPS 199 by assessing the impact of a compromise on the confidentiality, integrity, and/or availability of the federal data held within the system and require contractors to implement security controls from the corresponding baseline of the current version of NIST SP 800-53 as well as any additional security or privacy controls specified by the agency from NIST SP 800-213 (IoT *Device Cybersecurity Guidance for the Federal Government)*; NIST SP 800-161 (*Cybersecurity Supply Chain Risk Management Practices for Systems)*; and Organizations, and NIST SP 800-

82 (*Guidance to Industrial Control Systems Security)*. The rule would also require contractors to:

- Assist the Government in carrying out a program of inspections of the information system to safeguard against "threats and hazards" to the security and privacy of Government data or require the contractor to: (i) provide the Government (including CISA for civilian agencies) with "timely and full" access to Government data and "Government-related data;" and (ii) timely access to contractor personnel and facilities involved in the performance of the contract;
- Comply with Binding and Emergency Operational Directives ("BODs" and "EODs") issued by CISA that have specific applicability to a FIS used or operated by the contractor;
- Develop System Security Plans and Contingency Plans for all applicable FISs;
- For Moderate and High Impact Systems: Conduct annual threat hunting and vulnerability assessments; and Conduct an *annual independent assessment* of the security of each FIS and submit the results of these assessments to the contracting officer, and implement recommended improvement or remediations based upon the results of this annual assessment;
- *Report cyber incidents and cyber threats* to the appropriate authorities pursuant to the requirements included in FAR 52.239-ZZ (FAR Case 2021-017 described above);
- Provide cryptographic key materials to the federal agency; and
- *Document the scope of Operation Technology ("OT")* systems in use within the system boundary and provide a list of these systems as well as information on certain controls relating to their password requirements and remote access capabilities to the federal agency.

FAR Clause 52.239-YY would require agencies to categorize FISs as Low, Moderate, or High impact using FIPS 199 and the corresponding Federal Risk and Authorization Management Program ("FedRAMP") authorization level. Contractors will be required to

implement the corresponding controls for the FedRAMP authorization level (Low, Moderate, or High) for all cloud computing services delivered under the contract.

For systems which are categorized as High Impact, the contractor is required to physically maintain the system and associated Government data and Government-related data within the United States or its outlying areas.

While these proposed FAR Clauses mirror existing NIST Risk Management Framework ("RMF") and FedRAMP requirements, they expand federal agency and regulator access to contractor information systems as well as implement new data sovereignty requirements for high impact cloud computing systems operated on behalf of federal agencies. They also explicitly reinforce the expansive and stringent access and reporting requirements contained in FAR Case 2021-2017 increasing the need for timely and fulsome cyber incident and threat identification and reporting.

XIV. Conclusion

2023 has brought with it a flood of new cybersecurity and privacy regulations. 12 U.S. states have adopted comprehensive data privacy laws that started going into effect in January of this year.[68] The Biden Administration's new National Cybersecurity Strategy is calling for legislation to hold companies liable for failures to implement minimum cybersecurity standards, new FAR proposed rules would significantly increase the costs of doing business with the government requiring cybersecurity incidents to be reported to the government within eight hours (far less than any other regulation and before companies even likely have time to conduct preliminary assessments of the incident), and at the time of this writing, CMMC 2.0 proposed rules are expected soon. DOJ has made clear through its settlements, prosecutions, and statements that they consider cybersecurity and data security compliance a top priority. Liability for submitting false claims to the government is not limited to civil liability under the FCA but could also give rise to criminal liability under numerous federal criminal statutes, including 18 U.S.C. §§ 286-287 (making false or fraudulent claims and conspiracy to defraud the government with respect to claims), 1001 (making materially false statements to the government or concealing material information from the government), 1343 (wire fraud), and 1349 (conspiracy to commit wire fraud). The

SEC and FTC have similarly been cracking down on lax cybersecurity and misleading disclosures concerning data breaches.

There are no shortcuts or quick solutions that can be adopted to avoid becoming a target of a federal or state enforcement action. Rather, organizations need to properly safeguard data, implement a strong cybersecurity program that complies with reasonable industry standards such as NIST SP 800-171, and provide extensive training about cyber controls. Further, it is critical that organizations promptly respond and investigate any complaints regarding cybersecurity and privacy violations.

Although a cybersecurity incident by itself is not sufficient to create FCA liability, DOJ will likely prioritize bringing FCA actions for knowingly failing to report a cyberattack. This should not come as a surprise. First, DFARS Section 7012 has required defense contractors that possess CUI to report cyber incidents to DOD within 72 hours for years. Second, as noted above, one of the primary purposes of DOJ's Civil Cyber-Fraud was to encourage reporting of cyberattacks. Similarly, the prosecution of Sullivan, Uber's former CSO, stemmed, in large part, from his actions to conceal a hack of a massive amount of personal information so criminal liability could also result from concealing or obstructing a hack of CUI or personal information. Third, weak cybersecurity is jeopardizing both our national security and military advantage.

An IRP is essential to increase your organization's agility and nimbleness in responding to a cybersecurity incident so that you can comply with federal regulatory requirements, contractual obligations, minimize losses, mitigate vulnerabilities, restore operations, and strengthen your security to prevent similar cyberattacks in the future. Yet, more than one-third of organizations do not have an IRP.

When a breach occurs, your business will need to quickly determine whether personal or sensitive data has been compromised and make legal and contractual notifications within required time frames. An organization's failure to do this may result in substantial, and avoidable, liability and penalties. According to IBM's 2023 Cost of Data Breach Report, the average total cost of data breach is $4.45 million, the cost of a ransomware attack (not including the cost of the ransom itself) is $5.13 million, and the most common causes of a data breach are phishing and the use of stolen or compromised

credentials. These numbers are staggering but your organization can significantly reduce the impact of a data breach or cybersecurity incident and also reduce the threat of both criminal and civil liability by implementing a CIRP and creating a culture of cyber resilience and preparedness. Companies that have a CIRP save on average $2.66 million in responding to a data breach. Companies that have a CIRP, have instituted comprehensive cybersecurity training, conduct table-top exercises of their CIRP, and employ endpoint detection and response security greatly reduce and minimize the damages resulting from cyberattacks or accidental/negligent cybersecurity incidents caused by corporate insiders or vendors.

---

[1]Although the numbers are imprecise because there are currently no uniform requirements to report cyberattacks, numerous studies and reports have concluded that more than 50% of companies have experienced some form of a cyberattack in the last 12 months and one study found that 94% of organizations across 14 countries experienced a cyberattack in the last year. *See* Sophos Whitepaper, published April 4, 2023 available at http://www.sophos.com/en-us/whitepaper.state-of-cybersecruirty.

[2] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023) at 10, available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[3] *See* Joint Cybersecurity Advisory, *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* (June 2023), https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF.

[4] *See The Chinese Groups Accused of Hacking the US and Others*, Reuters, Jul. 21, 2023, available at https://www.reuters.com/world/china/chinese-groups-accused-hacking-us-others-2023-07-21/.

[5] *See* Warren P. Strobel, et al., *Beijing Plans a New Training Facility in Cuba, Raising Prospect of Chinese Troops on America's Doorstep*, Wall Street Journal, June 20, 2023, available at https://www.wsj.com/articles/beijing-plans-a-new-training-facility-in-cuba-raising-prospect-of-chinese-troops-on-americas-doorstep-e17fd5d1.

[6] *See id.*

[7] A Zero Day vulnerability is a vulnerability where the system or software vendor is not aware of the vulnerability and no patch exists, making it the most severe vulnerability an information system can face. A Zero Day attack is an exploit of a Zero Day vulnerability.

[8]*See Microsoft Digital Defense Report 2022*, available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

[9] *See* Michael Martina, *U.S. Warns New Chinese Counterespionage Law Puts Companies at Risk, Reuters*, June 30, 2023, available at https://www.reuters.com/business/us-warns-new-chinese-counterespionage-law-puts-companies-risk-2023-06-30/.

[10] Jill Goldenziel, *China's Anti-Espionage Law Raises Foreign Business Risk*, Forbes, July 3, 2023, available at https://www.forbes.com/sites/jillgoldenziel/2023/07/03/chinas-anti-espionage-law-raises-foreign-business-risk/?sh=cc623fe769ee.

[11] *Id.*

[12]While Russia has denied involvement, both the U.S. and U.K. intelligence agencies have attributed this attack to Russia. Journalist Andy Sandberg has further attributed these attacks to the Russian APT group known as "Sandworm."

[13]The fraudulent practice of sending emails or other messages purporting to be from a reputable source in order to deceive people into revealing sensitive information, trick people into downloading malware, or directing them to take other actions that expose themselves or their organizations to cybercrime. Often, the phishing email induces individuals to reveal personal or business information such as user credentials like usernames and password or log-in information, biographical data, or financial information such as bank account or credit card numbers. Successful phishing attacks often lead to identity theft, credit card fraud, data breaches, and ransomware attacks.

[14] *See FBI 2022 IC3 Report*, available at http//www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

[15] *See id.*

[16] Robert McMillan and Dustin Volz, *How North Korea's Hacker Army Stole $3 Billion in Crypto, Funding Nuclear Program*, Wall Street Journal, June 11, 2023, available at https://www.wsj.com/articles/how-north-koreas-hacker-army-stole-3-billion-in-crypto-funding-nuclear-program-d6fe8782.

[17] *See Financial Crimes Enforcement Network's Financial Trend Analysis: Business Email Compromise in the Real Estate Sector*, released April 2023, available at http//www.fincen.gov/sites/default/files/sahred/Financial_Trend_Analysis_BEC_FINAL.pdf.

[18] *See* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev.2 at 21 (2012).

[19] *See* 50 U.S.C. §1705(c) (willfully violating, attempting or conspiring to violate, or causing another person or entity to violate an Executive Order or OFAC regulation carries a maximum penalty of imprisonment for 20 years and a $ 1,000,000 fine for each violation).

[20] *See* www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[21] CISA, *Security-by-Design and –Default* (June 12, 2023), https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default.

[22] *See Merck & Co, Inc. v. Ace American Ins. Co.*, No. A-1879-21 (May 1, 2023 N.J. App. Div.).

[23] *See* Press Release, U.S. SEC, *SEC Charges Issuer with Cybersecurity Disclosure Controls Failures* (Jun. 15, 2021), https://www.sec.gov.news/press-release/2021-102.

[24] *See* Press Release, U.S. SEC, *SEC Charges Pearson plc for Misleading Investors About Cyber Breach* (Aug. 16, 2021), https://www.sec.gov/news/press-release/2021-154.

[25] *See* Press Release, U.S. SEC, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors* (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48 ("SEC BlackBaud Press Release").
[26] *Id.*

[27] *See* SEC Complaint and Order Instituting Cease-and-Desist Proceedings against Blackbaud (Mar. 9, 2023) at 2, https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf ("SEC Blackbaud Complaint").

[28] *Id.*

[29] *See* SEC Blackbaud Press Release.

[30] *See* SEC Blackbaud Complaint at 4.

[31] *See id.* at 2-5.

[32] Reuters, *SolarWinds Executives Receive Wells Notice from US SEC*, June 24, 2023, available at https://www.reuters.com/technology/solarwinds-executives-receive-wells-notice-us-sec-2023-06-23/.

[33] *See* SEC's Enforcement Manual at § 2.4, released Nov. 28, 2017, available at https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. The Wells Notice identifies the securities law violations that the SEC staff has preliminary determined will be included in their recommendation and provides notice that the targets may make a submission to the SEC concerning the proposed recommended charges. *Id.*

[34] U.S. Government Accountability Office WatchBlog, *SolarWinds Cyberattack Demands Signficant Federal and Private-Sector Response* (posted April 22, 2021), available at https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[35] *See* SEC Final Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Report Disclosure by Public Companies, available at https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

[36] *See id.*

[37] *Id.* at 29-30.

[38] *Id.*

[39] *See* SEC proposed cybersecurity rules, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[40] *See* Rapid7 Comments to SEC Proposed Cybersecurity Rules (Aug. 29, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20137661-308069.pdf.

[41] *Id.*

[42] These proposed regulations must be published by 2024 and CISA must issue a Final Rule setting forth the regulatory requirements within 18 months of the publication of the Notice of Proposed Rulemaking. *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022 Fact Sheet, available at https://cisa.gov/resources-tools/resources/cyber-incident-reporting-critical-infrastructure-act-2022-fact-sheet.

[43] *See* Press Release, U.S. FTC, *Commercial Surveillance and Data Security Public Forum* (Sept. 8, 2022), https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.

[44] *See* Press Release, U.S. FTC, *Fortnite Video Game Maker Epic Games to Pay More than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

[45] *See* Press Release, U.S. FTC, *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras* (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users; Press Release, U.S. FTC, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Viocie Recordings Forever and Undermining Parents' Deletion Requests* (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[46] *See* Press Release, U.S. DOJ, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[47] 143 S.Ct. 1391, *1399, Nos. 21-1326 and 22-111 (June 1, 2023).

[48] *Id.* at *1401.

[49] *Id.* at *1404.

[50] *See* Press Release, U.S. DOJ, *Medical Service Contractors Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Service Contracts at State Department and Air Force Facilities in Iraq and Afghanistan* (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

[51] *See United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245-WBS, 2022 WL 297093, *7-8 (E.D. Cal. Feb. 1, 2022).

[52] *Id.*

[53] *Id.* at *7.

[54] *Id.* at *5-7.

[55] *Id.* at *8.

[56]*See* Press Release, U.S. DOJ, *Aerojet Agrees To Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Contracts* (Jul. 8, 2022), https://www/justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resovle-false-claims-act-allegations-cybersecurity.

[57]*See* Speech, *DAG Monaco Delivers Keynote Address at International Conference on Cyber Security* (Jul. 19, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-address-international-conference.

[58]*See* Press Release, U.S. DOJ, *Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website* (Mar. 14, 2023), https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability.

[59] *See* Government Sentencing Memorandum filed in *U.S. v. Joseph Sullivan*, No. 3:20-cr-00337-WHO (Apr. 27, 2023).

[60] See Press Release, U.S. DOJ, *Former Chief Security Officer of Uber Convicted of Federal Charges for Covering Up Data Breach Involving Millions of Uber User Records* (Oct. 5, 2022), https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.

[61] James Rundle, *Prosecution of Former Uber Security Chief Carries Warnings for Cyber Leaders*, Wall Street Journal (May 5, 2023), available at https://www.wsj.com/articles/former-uber-security-chief-gets-probation-in-obstruction-case-87c7c0b9.

[62] The 9/11 Commission Report (Aug. 21, 2004), https://9-11commission.gov/report.

[63] *Id.* at 419.

[64]*See* 32 C.F.R. § 2022.1(f) ("This part applies to all executive branch agencies that designate or handle information that meets the standards for CUI. This part does not directly apply to non-executive branch entities, but it does apply indirectly to non-executive branch CUI recipients, through incorporation into agreements…").

[65] FedRAMP is a government-wide federal program for agencies to grant an Authority to Operate ("ATO") to cloud service providers who will operate an IT system on behalf of an agency. This involves a nonfederal Third-Party Assessment Organization ("3PAO") conducting an independent

audit of the applicant's system with the results submitted to the agency Authorizing Official ("AO") who would then make a risk-based decision on whether the agency would procure the system. The FedRAMP process also offers a Joint Authorization Board ("JAB") provisional ATO which is granted by the primary governing body of FedRAMP.

[66] NIST SP 800-171, SP 800-171A, SP 800-172, and SP 800-172 form what is called the "CUI Series" and represent the sum total of NIST efforts to provide federal agencies with standards and assessment procedures to provide varying levels of assurance that CUI is protected when shared with nonfederal entities.

[67]DOD Instruction 5230.25 (1984) gave initial guidance on protecting export controlled technical data (pursuant to the Arms Export Control Act) and contractor proprietary data from public release. DOD Directive 5230.24 (1984, updated in 1987, 2012, and 2023) first instituted agency procedures for marking unclassified technical data with distribution statements (A-F, X).

[68]The United States has taken a patchwork approach to data privacy with the potential of each state creating a different set of rules similar to the 50 different data breach laws that currently exist. This has resulted from the lack of one comprehensive federal law that governs data privacy. These laws increase the potential for criminal and civil liability by state enforcement actions. While most of these laws do not contain a private right of action, class action lawsuits are increasingly being brought for violations of both data security and privacy laws.