Navigating the SolarWinds Supply Chain Attack

By Evan D. Wolff, Kate M. Growley, Maida O. Lerner, Matthew B. Welling, Michael G. Gruden, and Jacob Canter

Evan D. Wolff

Kate M. Growley

Maida O. Lerner

Matthew B. Welling

Michael G. Gruden

Jacob Canter

The SolarWinds supply chain attack is a significant cybersecurity attack with widespread domestic and international effects. Perhaps the most significant aspect of the attack is the breadth of its effects, impacting both government and commercial organizations and creating historic impacts that will likely define future obligations and expectations for a broad array of contractors of all sizes and sectors. For that reason, it is important for government contractors to understand the nature of the incident and its impact. The following sections discuss (1) what we know currently about the attack, (2) guidelines for the incident investigation and response phase, (3) a use case of potential notification obligations triggered by an incident, (4) a framework for supply chain risk assessment and risk mitigation, and (5) information-sharing opportunities. Following these sections, we have included a checklist that may help guide contractors through each step of incident response and remediation for addressing the potential impact of the SolarWinds attack.

Evan D. Wolff is a partner in the Washington, D.C., office of Crowell & Moring. He co-chairs the Privacy & Cybersecurity group and is a member of the Government Contracts group. Kate M. Growley (CIPP/US, CIPP/G) is also a partner in Crowell & Moring's Washington, D.C., office. She is a member of the Steering Committee for the firm's Privacy & Cybersecurity Group and works closely with the firm's Government Contracts and Litigation groups. Maida Lerner is senior counsel in Crowell & Moring's D.C. office and a part of the firm's Privacy & Cybersecurity, Government Contracts, and Environment & Natural Resources groups. Matthew B. Welling is a counsel in the D.C. office, where he practices in the Privacy & Cybersecurity and Energy groups. Michael Gruden (CIPP/G) is an associate in the D.C. office and a member of the firm's Government Contracts and Privacy & Cybersecurity groups. Jacob Canter is an associate in the San Francisco office of Crowell & Moring. He is a member of the Litigation and Privacy & Cybersecurity groups.

Background

The Attack

The malicious software (malware) used in the SolarWinds supply chain attack is known as SUNBURST.[1] SUNBURST can lay dormant and hidden when inactive, but when activated can create "backdoors" that allow third parties to enter a software ecosystem without permission. This is significant because once a backdoor is created, the threat actors who initially planted the malware can use it to establish additional persistent access to the infected system and, from that, work to move elsewhere in the network, establish additional persistence, and conduct other malicious activities—in many cases even if the malware itself is removed.

SUNBURST was injected into SolarWinds Orion IT management software. At present, the earliest evidence of unauthorized access to the SolarWinds code is September 2019.[2] Once embedded in the Orion software, the malware was pushed into enterprise ecosystems as a part of otherwise legitimate SolarWinds software updates. These updates were not detected in part because the malware was so effectively hidden, and also because the updates bore digital indicia that usually evidence reliability (i.e., they were pushed through the legitimate SolarWinds software update process). The earliest-known corrupted update was pushed over 12 months ago, in March 2020.[3]

While the SolarWinds supply chain has been the most publicly visible component of this attack, contractors that do not use SolarWinds Orion have also been

impacted by these attackers. For example, it appears that some contractors may have been impacted through third parties with access to their network—cybersecurity vendor CrowdStrike has publicly stated that it does not use SolarWinds tools and its network was attacked through a Microsoft reseller.[4] Malwarebytes, which produces antivirus and other cybersecurity tools, has also publicly stated that it was a victim of these attackers but that it also does not use SolarWinds tools.[5]

The threat actors behind these attacks are highly sophisticated, both in terms of their attack planning and coordination and also in terms of their deep knowledge of key components of the environments they are targeting. Not only were they able to successfully compromise the SolarWinds supply chain with malicious updates; they have also been documented as having performed a substantial number of well-orchestrated activities once inside a victim environment, including moving laterally within that ecosystem, creating new access points into a system, compromising or establishing system accounts, overcoming authentication mechanisms, and changing application permissions. Industry experts commenting on the attacks have emphasized their complexity, and likely the significant financial investment of each victim attack, as well as how each intrusion is highly bespoke to the particular target (which is highly unusual because of the time and resources that requires).[6]

The tactics, techniques, and procedures (TTPs) of these threat actors further demonstrate their sophistication and how well-resourced these attacks have been. As an example, the threat actors' manipulation and use of unauthorized Security Assertion Markup Language (SAML) tokens is notable. Their use of SAML tokens has been observed as allowing them to move freely within even mature, well-instrumented environments without immediately raising red flags, including email services, business intelligence applications, travel systems, timecard systems, and file storage services.[7] This is one of many aspects of these attacks that highlights the sophistication and deep knowledge behind the threat actors' ability to deftly penetrate and maneuver through victim environments without raising alarms.

The Office of the Director of National Intelligence, the FBI, the U.S. Department of Homeland Security (DHS), and the National Security Agency (NSA) have issued a joint statement formally declaring that Russia was most likely the origin of the attack.[8] Russia has denied involvement.[9]

The Impact

SolarWinds stated in SEC filings that up to 18,000 of its customers may have been infected through software updates.[10] While that may be the upper limit known at this time, other public information seems to indicate that the threat actors likely focused on a relatively small percentage of those potentially vulnerable environments. And the impacted systems do not appear to have been chosen at random. Rather, the threat actors appear to have been seeking sensitive information, particularly from the U.S. federal government, and targeted victims and systems likely positioned to directly or indirectly make such information accessible.[11] If we assume that this was the attack's objective, then the attack was arguably a success in several respects.

For example, as a consequence of the SolarWinds supply chain attack, email systems within the Treasury Department were reportedly compromised, and software at the Los Alamos National Laboratory, which makes and designs nuclear weapons for the federal government, were targeted as well.[12] Moreover, many of the private contractors that have publicly acknowledged being impacted—such as Microsoft, Cisco, Malwarebytes, Mimecast, FireEye, and CrowdStrike—are technology product and service providers that serve the U.S. government.[13] Though the precise information that may have been compromised by the threat actors is not publicly known, the mere fact that unauthorized actors plausibly had access to highly sensitive governmental information raises substantial risk, never mind the other less-sensitive information that may have also been exposed.

There are also significant details about the attack that remain unknown. Most notably, the extent of access that the threat actors were able to gain in impacted systems has not been disclosed in most cases, and the full extent of information that the attackers may have gained access to is also not clear at this time. In fact, even the total number and identities of the attackers' victims are not yet publicly known. In the short term, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has taken steps to monitor the situation and provide mitigation recommendations, as have key vendors including Microsoft, SolarWinds, FireEye, and others. While the long-term impact of the attack is not yet clear, it seems safe to say that we will be seeing the ripple effect of this attack for many years to come.

Investigation and Risk Mitigation

While the SolarWinds supply chain attack has certainly presented new challenges to contractors potentially impacted, directly or through their own supply chain, contractors should remember that the core tenets for investigating a potential cybersecurity incident still hold. First and most importantly, even though the SolarWinds supply chain attack is high profile, contractors should still follow their existing internal policies and procedures, to the extent those are in place. And whether through their policies or in the absence of them, contractors are well advised to adhere to industry best practices for incident investigations, for example, through well-established frameworks like the *Computer Security Incident Handling Guide* published by the National Institute of Standards and Technology.[14] Additionally, guidance from government and industry specific to this attack and threat actor should be incorporated into incident response efforts.

In terms of initial actions specific to the SolarWinds attack, if a company has not already done so, it should promptly determine whether SolarWinds Orion software is run anywhere within its enterprise. SolarWinds and government agencies, including CISA, have published guidance to help contractors determine whether a vulnerable version of the software is or was previously in use.[15] However, that check alone may not be sufficient because information released since this attack was first publicly identified indicates that the threat actor may have also utilized other entry vectors,[16] and, as noted above, some victims have indicated that they are not SolarWinds users.[17] In any case, if a contractor believes that there is an indication of a potential cybersecurity incident, it should consider initiating a privileged investigation led by legal counsel to ensure that appropriate protections are in place from the outset. This privileged investigation may include engagement of experienced technical consultants, who are often especially helpful to legal counsel when dealing with APT threat actors. This value is reflected in SolarWinds' attack-related guidance, especially for contractors that do not have such expertise in house.[18]

Once an investigation is initiated, the key technical path will typically be to hunt for indicators of compromise (IOCs) associated with this attack, as well as other evidence consistent with the threat actor's TTPs, and agencies like CISA and companies such as Microsoft and FireEye have published information to support contractors' efforts.[19] Contractors should also be ensuring that their security tools are up-to-date, properly configured, and running in order to detect known threats and to incorporate updates as they become available from vendors.

In coordination with the privileged technical investigation, contractors should also be working as appropriate to contain immediate threats, typically based on emerging findings from the investigation and also government and industry guidance.[20]

As the privileged investigation progresses, contractors will need to determine their potential risk exposure from the attack, generally taking into account factors such as the type and number of systems involved, the type and volume of data at risk, and impacts to their business.

Additionally, contractors should consider what getting to "safe" looks like for them, which can be a challenging exercise, to which experienced technical consultants may add value, when dealing with APT actors or other complex attacks.

Throughout the technical investigation and response, it will be important for contractors to follow appropriate guidelines and procedures for the collection and documentation of forensic evidence (typically directed by counsel in privileged investigations). It will also be important for them to take steps to preserve evidence and avoid loss (by, e.g., not powering assets if information in memory needs to be captured and ensuring that system logs are not lost during rollover).

In addition to technical steps, communications are a key component of incident response, especially for matters as high profile as SolarWinds. Where information is rapidly evolving, contractors' external communications need to stay accurate and consistent, though the level of detail may vary and evolve based on circumstances and the audience. Contractors should also be thoughtful about who will be tasked with communicating on behalf of the company and the channel to be used—ideally addressed as part of the company's incident response plan and related internal policies. Centralizing decisions about communications and messaging during the investigation phase is a good practice for any incident, but it is necessary when dealing with high-profile attacks like this. Responsible teams need to have clear guidance on how to handle incoming inquiries and how responses will be handled.

In addition to their own internal investigation, contractors should also review their supply chains for risk posed by this attack. While a handful of victim contractors have already been publicly identified, there are definitely more to come—e.g., Microsoft has indicated that it notified more than 40 of its customers that they were targeted or compromised.[21] Additional pointers for reviewing supply chain risk are provided further in the discussion below.

Looking forward, impacted contractors should be considering a number of legal issues in addition to those discussed in this section. Impacted contractors should be assessing their potential litigation risk related to this attack and should update assessments as additional information becomes known. Because of the nature of the attack and its potentially significant impacts, contractors should also consult with their counsel about whether to institute a blackout on stock sales for company insiders—including those involved in incident response.

Notification Obligations

A primary purpose of conducting a privileged investigation is to allow a contractor to identify the relevant facts, which can, in turn, inform how to interpret the contractor's legal obligations vis-à-vis those facts. Key among a contractor's legal decisions during incident response will be whether, when, and how to notify relevant stakeholders regarding the incident. For contractors, the precise terms of customer contracts will be critical in answering those questions.

Most customer contracts include some kind of reporting notification, but far fewer include standardized reporting requirements. The result is often a web of notification requirements that must be assessed on a contract-by-contract basis. The Department of Defense (DoD), however, presents a helpful—and common—use case for our purposes here. DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (the Clause), is a contract provision generally incorporated into all DoD contracts that includes specific notification requirements.

Its purpose is to ensure that contractors adequately

protect sensitive DoD information handled in performance of a contract. Although it appears in most defense contracts, the Clause applies only when the performance of the contract implicates "covered defense information" (CDI).[22] The Clause defines CDI as any information that meets all of the following criteria:[23]

- The information is described in the Controlled Unclassified Information (CUI) Registry, which includes but is not limited to controlled technical information and export-controlled information;[24]
- The information is marked, or otherwise identified in the contract, task order, or delivery order; and
- The information is either provided to the contractor by or on behalf of the DoD in support of performance of the contract or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract.

If a contractor is handling CDI under a contract, the Clause imposes extensive safeguarding requirements. Specifically, if a contractor processes, stores, or transmits CDI on its information system, it must implement "adequate security" on that system to protect the CDI.[25] When these security measures are nevertheless thwarted, the Clause also requires that a contractor report certain events to the DoD that could compromise the confidentiality of CDI. Specifically, a contractor must report "cyber incidents" that "affect" CDI or any information system on which CDI resides.[26]

The Clause broadly defines a "cyber incident" as any action "taken through the use of computer networks that results in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."[27] A "compromise" is defined as a "disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred."[28] Importantly, the Clause does not formally define what constitutes a cyber incident that "affects" CDI.

The potentially broad reach of the Clause's reporting triggers adds to the array of decisions that must be made in response to incidents like the SolarWinds supply chain attack. And such decisions must often be made quickly. A contractor (or subcontractor) must report such incidents to the DoD through the DIBNet portal[29] within 72 hours of discovery.[30] Adding to the timeline is that use of the portal requires a DoD-approved medium-assurance certificate.[31]

Required information for an incident report typically includes:[32]

- company contact information;
- a Data Universal Numbering System (DUNS) number;
- contract numbers (or other type of agreement) potentially affected;
- contracting officer and government program manager contact information;
- contract and facility clearance level;
- facility CAGE code;
- impact to CDI and/or ability to provide operationally critical support;
- date incident discovered;
- locations (including CAGE code) of compromise;
- DoD programs, platforms, or systems involved;
- type of compromise;
- description of technique or method used;
- incident outcome;
- incident narrative.

Upon submission of a report, the DoD provides the contractor with an "Incident Collection Form" number, and the contracting officers identified in the report are notified.[33] Where an incident implicates multiple contracts, as is likely to be the case under the SolarWinds supply chain attack, the DoD designates a single contracting officer to coordinate with the contractor.[34] Importantly, a contractor who is unable to provide all of the required information within the 72-hour timeline must supplement the initial report as soon as the outstanding information becomes available.[35] If a contractor can isolate malicious software related to the incident, it may be asked to separately submit a sample of the malware to the DoD Cyber Crime Center.[36]

The obligations do not stop there. The contractor must also preserve and protect images of all information systems known to be affected, as well as all relevant monitoring/packet capture data, for 90 days from the date on which the report was submitted.[37] Based on the report, the DoD may elect to conduct a damage assessment, in which case it may request this preserved data. If requested, the contractor must provide the DoD with access to any other information or equipment that is necessary for the DoD to conduct a forensic analysis as part of the damage assessment process. Additionally, the DoD may request an assessment of the contractor's compliance with the Clause's "adequate security" requirements.[38] Notably though, the fact that the contractor has reported a cyber incident does not, by itself, automatically establish that the contractor has failed to meet its security obligations under the Clause.[39]

These provisions of the Clause allow access to a potentially extensive scope of contractor information. To mitigate the resultant risks, the Clause requires the DoD to protect a contractor's attributional and proprietary information from unauthorized use or release.[40] Notably though, the Clause does not specify what these protections are. It does, however, include a long list of circumstances in which the DoD may release a contractor's attributional or proprietary information. Many of these circumstances could be relevant in the context of the

SolarWinds supply chain attack, such as those in which the information is released:

- to entities with missions that the information may affect;
- to entities assisting in the diagnosis, detection, and/or mitigation of cyber incidents, including those supporting the DoD's assessment of the specific cyber incident at issue;
- to government entities that conduct counterintelligence or law enforcement investigations; or
- for national security purposes, including cyber situational awareness and defense purposes.[41]

Although the precise terms of customer contracts will vary, they are likely to reflect at least some of the issues necessary to consider in the context of the Clause here.

Incoming Information Sharing/Directives

During incidents, contractors should not focus solely on identifying what is happening internally. Rather, they should also be equipped to receive and gather information security updates from external sources, which can provide timely information regarding security patches and related guidance. Such sources typically include government agencies (e.g., CISA), as well as the broader information technology commercial sector. Moreover, all information shared should not be received with equal credence. Government directives should generally receive greater attention and adherence, while industry guidance should be treated as industry best practices.

The response to the SolarWinds supply chain attack represents one of the best examples of effective information sharing between the U.S. government and industry, as well as data exchange between industry peers. Following the identification of this attack, CISA, a DHS component agency focused on managing cybersecurity risks within the nation's critical infrastructure, led through successive release of Emergency Directives regarding the incident.[42] The initial Directive instructed federal civilian agencies to "review their networks for indicators of compromise" regarding SolarWinds Orion products.[43] An indicator is considered a "sign that an incident may have occurred or may be currently occurring,"[44] while a compromise is an "unauthorized disclosure, modification, substitution, or use of sensitive information."[45]

CISA provided supplemental guidance where it directed agencies to utilize version 2020.2.1HF2 of the SolarWinds Orion platform, for which the NSA verified that the malicious code had been eliminated.[46] Subsequent guidance required agencies to (1) conduct forensic analysis, (2) comply with cybersecurity hardening requirements, and (3) report agency status to CISA.[47]

The Emergency Directives provided by CISA were not entirely unique because DHS has taken decisive action in the past when threat levels rose to a significant magnitude. In 2017, DHS issued a Binding Operational Directive (BOD)[48] requiring all federal agencies to remove and discontinue use of all Kaspersky antivirus software after the discovery of potential Russian government threat actors.[49] The Kaspersky BOD and SolarWinds Emergency Directives alike should catch the attention of government contractors because contractors would arguably be required to implement such directives when they are operating a federal information system on behalf of the government.

Supply Chain Risk Management

The SolarWinds supply chain attack demonstrates in stark terms the importance for contractors, especially government contractors, to manage and take steps to mitigate cybersecurity supply chain risk. Due to the nature of their businesses, prime and higher-tier contractors are subject to a wide variety of cybersecurity laws, regulations, and standards, as well as policy and contractual obligations, at all levels of government, relating to the protection of sensitive and proprietary government and business information. Many of these laws, regulations, and standards focus on prime contractors' supply chains and impose obligations through contractual provisions.

Here, too, the previously discussed DFARS Clause 252.204-7012 provides a helpful use case: Its safeguarding and cyber incident reporting obligations must be flowed down to subcontractors that are expected to handle CDI.[50] Moreover, a recently published Interim Rule[51] further provides that a prime contractor may not award a subcontract unless the subcontractor has a current assessment in the Supplier Performance Risk System (SPRS).[52] This heightened government attention to managing cybersecurity supply chain risk is due primarily to the increased risk to contractors from cyberattacks and the fact that each level of the government contracting chain is a potential point of cyber risk for the government customer.

Challenges facing contractors to manage and mitigate supply chain risk typically fit within three areas. First, contractors often do not have a full and current inventory of which of their subcontractors have access to sensitive data and information and how those data and information are being protected. Data mapping, especially for global contractors, may be a resource-intensive and complex task. Second, many contractors do not have an established process for assessing risk even once they understand where sensitive information resides or how it is used by subcontractors. Third, contractors may not yet have developed a risk-based and cybersecurity supply chain risk mitigation and remediation strategy despite the potentially significant consequences of failure to act.

Recognizing that it may not be possible to eliminate all supply chain risk as cyber threats evolve, the following are risk-based activities that contractors may consider to mitigate and remediate potential risk to a level acceptable for your company.

1. Survey the Supply Chain

Generally, a necessary first step in managing supply

chain risk is to gather information. Contractors may consider surveying subcontractors who have access to the company's technical data and other sensitive and proprietary information to determine the baseline security posture of those suppliers. Some government contractors use the Exostar Partner Information Manager (PIM) tool, a risk management tool that leverages information from trusted resources to provide a partner with a supplier's current and potential risk and impact. These surveys are often supplemented through conference calls with key suppliers and on-site visits.

Other information collection tools used by government contractors may include Endpoint Detection and Response (EDR) tools and insider threat toolsets that work with IT and human resource–based systems to detect potential insider threats from the supply chain.

2. Analyze the Information Gathered

Using the information gathered, a contractor should be better equipped to analyze each of its subcontractors' current compliance posture. This analysis will address, as appropriate, compliance with applicable regulatory requirements, the relevant policies and contractual obligations, and industry best practices. As part of these efforts, the contractor may continue to have and to document follow-up discussions with its subcontractors.

3. Implement Risk Mitigation and Remediation Actions

Finally, a contractor, armed with the compliance assessment, may act to remediate any identified cybersecurity supply chain risk. Follow-up actions will typically be informed by legal obligations as well as by the criticality of the subcontractor. In other words, a contractor may invest resources to critical suppliers that it may not to others. Some attributes that may be used as guides in determining the criticality of a supplier may include whether the supplier is a sole/single-source supplier, whether the supplier has "crown jewel" information, the volume or spend for the supplier relative to the total supplier population, whether the supplier supports multiple programs or a key program (as determined by the customer), or whether this is a high-value strategic partner.

Options offered by contractors to help critical suppliers mitigate cyber risk may include offering cybersecurity education and awareness training, appropriate oversight and assessment of the subcontractors' compliance program, and improved supplier management. In addition, to address potential risk of critical suppliers, a contractor may consider work-arounds. For example, in addressing DFARS Safeguarding Rule requirements, if it is determined that a subcontractor needs access to CDI to perform its functions but is unable or unwilling to comply with the flow-down requirements included in the Clause, the contractor may consider offering a hard copy of the CDI to the subcontractor in lieu of electronic access or offer guest accounts on the contractor's network for the supplier to access the information. If these "alternatives" are offered, a contractor may also consider reasonable restrictions on the subcontractor's use of the hard copy or read-only access to mitigate potential risk. For example, contractual provisions may be considered that require the supplier to not download, re-create, or allow CDI on its network; protect the information in its possession; and either return the information to the contractor or destroy it when performance is complete.

In contrast, for noncritical subcontractors, if the subcontractor refuses to take the necessary steps to achieve compliance, the contractor may consider terminating the relationship.

Bringing It All Together: A Checklist

Contractors may consider referencing this checklist as an informal guide for cybersecurity incident response associated with the SolarWinds supply chain attack.

Initial Actions

Check for SolarWinds

Does your company run SolarWinds Orion anywhere in the enterprise? Check guidance from SolarWinds, the Cybersecurity and Infrastructure Security Agency (CISA), and other government entities to determine if vulnerable versions were in place during the attack's time frame.

But It's Not Just SolarWinds

Because information about this attack continues to develop, contractors should not assume that no further action is needed if SolarWinds is not present. Continue to monitor updates to reevaluate whether further action is warranted.

Privileged Investigations

If a vulnerable version of SolarWinds Orion is present or other information indicates compromise, consider initiating a privileged investigation led by counsel.

Your Network

Hunt for IOCs and TTPs

Potentially impacted companies should hunt for indicators of compromise (IOCs) as well as for evidence consistent with tactics, techniques, and procedures (TTPs) identified as part of this attack. Government entities and security vendors have released this information, and further updates are expected.

Update Security Tools

Ensure that security tools are up-to-date, properly configured, and running. Security vendors have been releasing product updates to improve detection and/or prevention as more information on IOCs and TTPs becomes known.

Determine Potential Exposure

While the full nature and impacts of this attack are still developing, potentially impacted companies should determine the scope of exposure they may face, including systems involved, data at risk, and business impacts.

Contain the Threat
Consult current guidance for recommended actions. For example, CISA Emergency Directive 21-01 called for capturing forensic images of systems with vulnerable SolarWinds versions, then immediately disconnecting or powering down.

Logs
Make sure all log sources for the full timeline for the attack are available for analysis. Companies may need to collect logs from multiple sources, and some may need to be restored or unarchived for coverage back to the initial incident time frame.

Preserve Evidence
Prompt action may be necessary to contain threats, but failure to preserve forensic evidence in doing so may limit subsequent investigation. For example, powering down a system before capturing a forensic image may lose information in memory.

Getting to Safe
Eradication of APT threats and subsequent recovery typically require an iterative process and varying levels of "safe." Determining whether systems are "safe" and what "safe" means at a given point is often difficult, which is why government and security vendors are recommending that companies work with professionals with APT experience.

Forensic Vendors
If companies do not have significant APT experience in house, third-party forensic vendors offer this expertise. For privileged investigations, current best practice is to engage vendors through counsel.

External Communications
Stay Consistent and Aligned
Especially in situations with evolving information, external communications need to stay accurate and consistent, although level of detail may vary and evolve as circumstances warrant. Companies should also be thoughtful about the individual or team tasked with communicating a given message and the channel to be used.

Centralize Decisions
Because the attack is high profile, companies should expect inquiries. Accordingly, companies should ensure that they have clear internal guidance on how incoming inquiries will be handled and how responses will be managed. Without this, the company risks ad hoc responses being made by unauthorized individuals and that leadership will not have visibility.

Statutory/Regulatory Obligations
The company also needs to be aware of statutory and regulatory obligations. Regulated industries may have mandatory reporting obligations for a potential compromise (e.g., healthcare companies under HIPAA), and publicly traded companies may need to make SEC disclosures for material impacts to their business. This includes whether impacts to their vendors trigger reporting obligations. Notification obligations may also be triggered if personal information or other types of regulated data were exposed by the attack (by, e.g., the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other U.S. state laws).

Contractual Obligations
The company needs to be aware of its contractual obligations related to a potential compromise, which may include notifications to impacted customers, vendors, or other counterparties. Government contractors should pay particular attention to reporting requirements built into their standard contractual clauses and statements of work. Depending on contracting practices, obligations, and their triggers, timing and form may vary.

Incoming Notifications
Companies should have clear internal guidance to ensure efficient and timely intake and escalation for notifications received that indicate potential impacts from the attack (e.g., from vendors, law enforcement/government, etc.).

Engaging with Law Enforcement/Government
Companies may opt to proactively engage with law enforcement or other government entities about this attack. Whether in response to a notification or proactive contact, all such communications should be coordinated with leadership and counsel.

Proactive Transparency
Companies may consider taking a more proactive and transparent approach to publicly disclosing cybersecurity incidents, which has been a recent trend and has already occurred with this attack. Additionally, security researchers are working to identify victims with attack information, which may create incentives to be proactive rather than reactive.

Supply Chain
Inquiries and Rights
Evaluate potential risk from this attack through the company supply chain, especially key vendors. The company should be prepared to undertake assurance efforts in an organized fashion to ensure consistency, efficient intake, timely response to identified risks, and appropriate documentation. The company should also clearly understand its contractual rights.

Risk Prioritization
Recognizing that vendors do not all present equal risk, companies should evaluate relative risks posed by each

vendor and address highest-priority risks accordingly (e.g., based on criticality, degree of network interconnectivity, or sensitivity of access). Such decisions should be made in a consistent and programmatic fashion, with appropriate involvement of leadership.

Additional Considerations

Internal Processes and Procedures

While this attack is high profile, companies should still follow applicable internal processes and procedures, including for governance and documentation. Departures may create unnecessary legal and business risk.

Intellectual Property Threats

This attack is already known to involve compromising SolarWinds code and stealing proprietary tools from FireEye. Potentially impacted companies should carefully review whether their IP has been impacted or is at risk.

Litigation Risk

Companies need to track their potential litigation risk associated with this attack, based on known potential impacts and in light of additional information that becomes known.

Stock Sale Blackout

Because of the nature of this attack and potential for significant impacts, companies should consult with counsel about whether to institute a blackout on stock sales for company insiders—including those involved in incident response. PL

Endnotes

1. *See SolarWinds Security Advisory*, SolarWinds, https://www.solarwinds.com/securityadvisory (updated Jan. 29, 2021).
2. *See Form 8-K Solarwinds Corp Current Report*, Sec. & Exch. Comm'n (Jan. 11, 2021), https://sec.report/Document/0001739942-21-000015/.
3. *See Threat Research: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, FireEye (Dec. 13, 2020), https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.
4. *See* Michael Sentonas, *CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory*, CrowdStrike Blog (Dec. 23, 2020), https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/.
5. *See* Marcin Kleczynski, *Malwarebytes Targeted by Nation State Actor Implicated in SolarWinds Breach*, Malwarebytes Blog, https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments/ (last updated Jan. 27, 2021).
6. *See, e.g.*, *Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, Cybersecurity & Infrastructure Sec. Agency, https://us-cert.cisa.gov/ncas/alerts/aa20-352a (last revised Jan. 7, 2021).
7. *See id.*
8. Press Release, Cybersecurity & Infrastructure Sec. Agency, Joint Statement by the FBI, CISA, ODNI, and NSA (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.
9. *See Embassy of Russia in the USA*, Facebook (Dec. 13, 2020), https://www.facebook.com/RusEmbUSA/posts/1488755328001519.
10. *See Form 8-K Solarwinds Corporation Current Report*, Sec. & Exch. Comm'n (Dec. 14, 2020), https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/0001628280-20-017451.txt (Document No. 0001628280-20-017451).
11. *See* David E. Sanger, Nicole Periroth & Julian E. Barnes, *As Understanding of Russian Hackings Grows, So Does Alarm*, N.Y. Times (Jan. 2, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.
12. *See* David E. Sanger, *Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect*, N.Y. Times (updated Jan. 2, 2021), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html; *see* Marie O'Neill, *DOE/NSA Responding to Cyber Incident Related to Solar Winds Compromise*, Los Alamos Rep. (Dec. 17, 2020), https://losalamosreporter.com/2020/12/17/doe-nnsa-responding-to-cyber-incident-related-to-solar-winds-compromise/.
13. *See* Brad Smith, *A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response*, Microsoft Blog (Dec. 17, 2020), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/; Marcin Kleczynski, *Malwarebytes Targeted by Nation State Actor Implicated in SolarWinds Breach*, Malwarebytes Blog (Jan. 27, 2021), https://blog.malwarebytes.com/malwarebytes-news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach-evidence-suggests-abuse-of-privileged-access-to-microsoft-office-365-and-azure-environments/; *Important Update from Mimecast*, Mimecast Blog (Jan. 12, 2021), https://www.mimecast.com/blog/important-update-from-mimecast/; FireEye, *Threat Research: Highly Evasive Attacker Leverages SolarWinds Supply Chair to Compromise Multiple Global Victims with SUNBURST Backdoor,* FireEye Blog (Dec. 13, 2020), https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html; Michael Sentonas, *CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory*, CrowdStrike Blog (Dec. 23, 2020), https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/.
14. Paul Cichonski et al., Nat'l Inst. of Standards & Tech., Dep't of Com., Computer Security Incident Handling Guide, NIST S.P. 800-61r2 (2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
15. *SolarWinds Security Advisory*, *supra* note 1; *Alert (AA20-352A)*, *supra* note 6.
16. *Alert (AA21-008A): Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments*, Cybersecurity & Infrastructure Sec. Agency, https://us-cert.cisa.gov/ncas/alerts/aa21-008a (last updated Feb. 4, 2021); Robert McMillan & Dustin Volz, *Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say*, Wall St. J. (Jan. 29, 2021), https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.
17. *See, e.g.*, Kleczynski, *supra* note 13.
18. *See, e.g.*, *Alert (AA20-352A)*, *supra* note 6 ("Take actions to remediate kerberoasting, including, as necessary or appropriate, engaging with a 3rd party with experience eradicating APTs from enterprise networks.").
19. *Alert (AA21-008A)*, *supra* note 16; *Solorigate Resource Center*, MSRC Blog (Dec. 21, 2020), https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/;

continued on page 28

continued from page 10

UNC2452 & Sunburst Resource Center: What Happened?, FireEye Blog, https://www.fireeye.com/current-threats/sunburst-malware.html.

20. *See, e.g.*, *CISA Updates Emergency Directive 21-01 Supplemental Guidance and Activity Alert on SolarWinds Orion Compromise*, Cybersecurity & Infrastructure Sec. Agency (Jan. 6, 2021), https://us-cert.cisa.gov/ncas/current-activity/2021/01/06/cisa-updates-emergency-directive-21-01-supplemental-guidance-and.

21. Brad Smith, *A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response*, Microsoft Blog (Dec. 17, 2020), https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

22. DFARS PGI 204.7304(c). The Clause also applies in limited circumstances where a contractor provides "operationally critical support." *See* DFARS 252.204-7012(c), (m).

23. DFARS 252.204-7012(a).

24. The complete Registry can be found at https://www.archives.gov/cui/registry/category-list.

25. DFARS 252.204-7012(b).

26. *Id.* at (c).

27. *Id.* at (a).

28. *Id.* A contractor must also report cyber incidents that affect the contractor's ability to provide "operationally critical support," as identified in the relevant contract. *Id.* at (c).

29 The DIBNet portal is available at https://dibnet.dod.mil/portal/intranet/.

30. DFARS 252.204-7012(c)(2).

31. *Id.* at (c)(3).

32. *See DIBNet Portal*, Def. Indus. Base Cybersecurity Info. Sharing Program, https://dibnet.dod.mil/portal/intranet/.

33. *See* DFARS PGI 204.7303-3(a), *Cyber incident and compromise reporting*.

34. *Id.* at (a)(2).

35. *Id.* at (d).

36. DFARS 252.204-7012(d).

37. *Id.* at (e).

38. DFARS PGI 204.7303-3(a)(3).

39. *Id.* at (d); DFARS PGI 204.7302(d).

40. DFARS 252.204-7012(h).

41. *Id.* at (i)(1)–(4).

42. *See CISA Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise*, Dep't of Homeland Sec. (Dec. 13, 2020), https://cyber.dhs.gov/ed/21-01/.

43. Press Release, Cybersecurity & Infrastructure Sec. Agency, CISA Issues Emergency Directive to Mitigate the Compromise of SolarWinds Orion Network Management Products, https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network (last updated Dec. 14, 2020).

44. *See* Cichonski et al., *supra* note 14, at 60.

45. *See* Elaine Barker & William C. Barker, Nat'l Inst. of Standards & Tech., NIST SP 800-57, Pt. 2, Rev. 1, Recommendation for Key Management 7 (May 2019).

46. *See CISA Emergency Directive 21-01*, *supra* note 42.

47. *Id.*

48. A BOD is a "compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems."

49. *See DHS Binding Operational Directive 17-01, Removal of Kasperksy-Branded Products*, Dep't of Homeland Sec. (Sept. 2017), https://cyber.dhs.gov/bod/17-01/.

50. DFARS 252.204-7012(c)(3).

51. Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61,505 (Sept. 29, 2020).

52. DFARS 252.204-7012(m)(2).