**Testimony of Katie Moussouris**

**Before the Committee on Science, Space, & Technology**

**Subcommittee on Investigations and Oversight & Subcommittee on Research and Technology**

**U.S. House of Representatives**

**On SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains**

**May 25, 2021**

**Washington, DC**

## Introduction

Chairman Foster, Ranking Member Obernolte, Chairwoman Stevens, Ranking Member Waltz, and distinguished members of the Subcommittees, thank you for inviting me to testify today about how to improve software supply chain security. My name is Katie Moussouris, I am the founder and CEO of Luta Security, a security company that works with governments and complex organizations to transform the way these organizations use people, processes, and technology to create mature, robust, and sustainable vulnerability disclosure and bug bounty programs. We base these programs on the industry international standards ISO/IEC 29147 Vulnerability disclosure[1], ISO/IEC 30111 Vulnerability handling processes[2], and our Vulnerability Coordination Maturity Model[3].

I am the co-author and co-editor of these international standards. I have more than 20 years of professional technical and strategic work in technology and information security, beginning as a penetration tester at @stake[4], followed by creating Microsoft Vulnerability Research, establishing Microsoft's first bug bounties, and advising the U.S. Department of Defense for several years, resulting in the launch of the Hack-the-Pentagon program. Additionally, I served as co-chair of the National Telecommunications and Information Administration's multi-stakeholder vulnerability disclosure working group subcommittee of multi-party vulnerability coordination[5]. I also served as one of two private industry official delegates of the U.S. technical experts working group to renegotiate the "intrusion software & intrusion software technology" provisions of the Wassenaar Arrangement[6], successfully helping clarify exemptions for vulnerability disclosure and incident response in export controls.[7] I am a cybersecurity fellow at New America and the National Security Institute, and I am also the founder of the Pay Equity Now Foundation[8].

1 https://www.iso.org/standard/72311.html

2 https://www.iso.org/standard/69725.html

3 https://www.lutasecurity.com/vcmm

4 https://en.wikipedia.org/wiki/@stake

5 https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf

6 https://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session

7 https://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global

8 https://www.payequitynowfoundation.org/

It is an honor to appear before these Subcommittees to testify about the challenges securing the software supply chain presents to our economy and our national security. While supply chain attacks have become more prevalent in the headlines during the past few years, these types of attacks have been occurring regularly since the dawn of major operating systems. Since the operating system (OS) sits fairly high upstream of most other technology, it has long been an effective target that is attacked, then used to compromise many downstream targets. This problem is not new and believing that it is can impede meaningful conversations regarding potential solutions.

The United States participates in the software supply chain in multiple complex roles, as do our international partners, and our adversaries. Taking on the challenge of securing the supply chain is not as simple as rolling out Executive Orders or even legislation but requires a nuanced approach that maximizes the investments in resources and capabilities we have, while measuring effectiveness and maturity, building new tools to scale solutions, and recruiting new talent to fill growing cyber security operational and strategic roles.

The COVID-19 pandemic and the move to remote work nearly overnight around the world drove more organizations to use technology to keep business operations going, often without increasing their cyber security budgets or personnel as they struggled with the economic downturn most businesses faced. Unfilled security jobs worldwide are over 3.1 million, with over half a million of those open roles in the United States[9]. This cyber workforce shortage has a compound effect when software supply chains are by definition interconnected, and only as strong as the weakest link upstream.

Our success in the desired outcome of improved cyber security, and greater cyber resilience, relies on our adaptability to threats and shifting tactics. Without a detailed understanding of our current capabilities, even our best intentions and efforts for following "best practices" and building new, world-leading capabilities will fall short of our adversaries' efforts more often than not. In the past year, "there was a 430% increase in upstream software supply chain attacks over the past year.[10]"

To address the complexity in software supply chain security, my testimony today will outline the problem space and offer proposed solutions and actions to measurably increase the cyber resilience of the United States and our international partners. I believe the following recommendations, building upon some of the most important work and best practices in the public and private sector, will increase our national security.

9 https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

10 https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf

1. Providing the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. Department of Homeland Security with the authorities and resources to oversee cyber readiness for the civilian federal government, and as a resource for promoting best practices and cyber security incident response consultative support for privately-owned critical infrastructure;
2. Amending FISMA to require an annual, comprehensive federal civilian agency gap analysis and maturity assessment that will identify critical gaps in people, process, and technology and also support maturity-based metrics, which will measure improvements in cyber security and cyber resilience;
3. Conducting a CISA-led survey of ROI for each proposed new requirement in the Cybersecurity Executive Order[11] to determine the priority of each based on the investments required to make a dent in the problem through a system dynamics analysis; and
4. Raising federal pay scales across the board in all roles, especially in cyber security, to better compete with the private sector, and investing in cyber security recruitment and training for existing and aspiring workers who require additional skills to support the cyber mission.

The United States government is not alone in having to reckon with the vast technical debt built up in the global supply chain. If we are to improve our cyber resilience and reduce our risk profile, we have to focus the hard work and investments in effective inflection points across the ecosystem, especially in the context of supply chain security.

**Understanding trends in supply chain attacks including SolarWinds**

There are multiple ways that supply chain attacks can occur, and not all efforts to combat these various attacks result in the same return on investment. In our ongoing national effort to build up our cyber resilience, we must evaluate the efforts put forth with desired outcomes in mind, to avoid overinvesting at this critical time in complex good ideas that might yield dividends down the line, versus doing the simplest measures that yield measurable increased security of the supply chain now.

While SolarWinds focused security efforts on compliance, their software build process was compromised resulting in the widespread attacks of their customers. SolarWinds had weak passwords found that were set by interns that were part of a larger organizational control failure that on the whole contributed to their overall missed security steps that allowed the supply chain attack to be planted, once the adversary gained access to their build pipeline. Weak passwords weren't the definitive smoking gun of how the attackers got in, but with low hanging fruit footholds like weak passwords allowed, and not enough internal segmentation, or integrity checks in the build process, the systems ended up silently compromised for months.

11 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The CodeCov[12] supply chain attack was similar, though so far it has garnered less attention in mainstream media. The attackers modified a CodeCov bash uploader to redirect credentials and other sensitive information, harvesting those downstream user's credentials and access tokens to further infiltrate the build processes of the downstream developers. It was insidious and the ramifications downstream are still not fully determined.

Smaller, ongoing supply chain attacks are usually overlooked until larger-scale attacks occur like the ones against CCleaner[13], and most recently, SolarWinds and CodeCov. Like most security problems, many experienced professionals seeing different angles of the problem envision different solutions for securing the software supply chain. One of the main reasons why these problems haven't yet been solved is that the cybersecurity industry itself is still in its infancy, while the United States and the world have grown exponentially faster in our dependence and complexity of increasingly interconnected technology.

During my 20 plus years as a cybersecurity professional, all the way back to my earliest modem-connectivity to the young Internet in the early 1990s, I have watched the scale of Internet defense grow at a slower pace than the emerging threats. Industry leading software manufacturing security best practices emerged by necessity, a wave of Internet worms regularly crippling early infrastructure, spawning the software giants to invest in their security response at first, followed by enhanced attack detection, and finally in incident prevention and resilience as they matured. This cybersecurity maturity has not had time to propagate to all software manufacturers, nor has it even taken root at some of the largest software builders, and it has no scalable support at some of the most heavily used open-source software deployed in systems worldwide.

As we have seen in the early software manufacturers who have matured in their software security capabilities, the downstream supply chain and the consumers of it, including the Federal government, must mature as well. In early stages of building our cyber resilience, we see organizations focus first on incident response, which has been echoed in the Cybersecurity Executive Order's breach notification requirements, as well as CISA's requests for more endpoint detection budget during recent Congressional hearings. Investing in better breach response is important, but the ROI for investment in breach prevention is higher yet lacks the urgency to drive near-term action.

One such maturation from pure security response into a broader supply chain vulnerability coordination focus was designed and implemented by me at Microsoft starting in 2008, when I created Microsoft Vulnerability Research (MSVR)[14] to look for vulnerabilities downstream in Microsoft's third-party software ecosystem and coordinate multi-party and supply chain issues in both hardware and software. Setting up this new multi-party and supply chain security capability was non-trivial, even for the largest software company in the world, investing in nearly half a billion dollars annually at the time in people, process, and technology that made up the organization formerly known as Trustworthy Computing.

12 https://blog.sonatype.com/what-you-need-to-know-about-the-codecov-incident-a-supply-chain-attack-gone-undetected-for-2-months

13 https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

14 https://www.microsoft.com/en-us/msrc/msvr

One of the first issues coordinated via MSVR was Dan Kaminsky's DNS vulnerability[15], which would have crippled the Internet. Another was a Microsoft Active Template Library (ATL) issue that affected all software compiled using that library downstream in the supply chain that also had to be coordinated in stages to enable protections to be rolled out to the most affected users at once. Yet another was a baseband chip family of issues that had to expand the coordination effort to most baseband chip manufacturers and standards bodies setting technical specifications.

One begins to appreciate the scale of the problem when even the largest organizations have only been tackling the issue of supply chain security head on for about a dozen years. While federal mandates can act as catalysts for positive change, unfunded mandates are less successful, and in this case, even well-funded new requirements will struggle to find skilled cyber workers to meet current and emerging needs.

**Challenges to both the private and public sector in responding to supply chain attacks**

We are, as a society, in a state of having built up interconnected cyber cities without enough cyber fire fighters, hydrants, or fire inspectors to ensure what we build next is safe. The infrastructure fragility caused by this chronic underinvestment in cyber security across both the federal and private sectors is at a crescendo now, not because supply chain attacks are new, but because they are increasing in frequency in parallel to the Internet resources upon which we increasingly depend.

Our federal and private sector capacity for responding to supply chain attacks and remediating underlying vulnerabilities is limited by gaps in people, process, and technology that change over time as new tools and processes are developed in the marketplace, and new workers are trained and gain experiences.

**Cyber workforce challenges in both public and private sector**

In an industry as young as cybersecurity, we do not have a good conduit for building a continuous pipeline of cybersecurity workers skilled at various levels to form a steady pipeline. The majority of security jobs are not entry level. Without providing entry-level jobs, mentoring programs, or training programs, we will never be able to effectively staff teams to prevent, detect, and remediate cyber attacks. The much-sought-after elite cyber workers that extremely well-funded organizations are seeking are cost-prohibitive for smaller private critical infrastructure organizations, as well as for federal, state, and local governments.

Even large organizations with many highly skilled technical workers struggle with getting the right resources in place to simultaneously respond to incidents and investigate and fix vulnerabilities. Security is not taught at most universities, and more successful coders come from diverse and informal backgrounds, compounding the issues of securing code, even if vulnerabilities are pointed out by skilled outsiders. The internal digestive system for vulnerabilities, as well as the muscle memory of an organization to handle its supply chain both upstream and downstream must be built over time.

15 https://channel9.msdn.com/Events/Blue-Hat-Security-Briefings/BlueHat-Security-Briefings-Fall-2008-Sessions-and-Interviews/v8-4

For example, while running two private bug bounty programs using outsourced support from both major bug bounty platform providers, Luta Security was called in to assist Zoom in the surge of new vulnerability report cases that came in when the pandemic created an exponential surge in popularity. Knowing about bugs is less than half the battle. We helped flatten the curve of Zoom's bug cases by 37 percent in less than 10 weeks, targeting and eliminating imminent zero-day risks for those cases. We also provided a vulnerability handling maturity gap analysis and roadmap for Zoom to use moving forward, as the company works toward achieving ISO 29147 and ISO 30111 compliance.[16]

To fill the gaps in the cyber workforce in the federal government, one issue to address is pay scale differences between the private and public sector, and another is to train new and existing federal workers. Raising federal pay scales across the board and especially in cyber security will allow for building out the more senior ranks of experts needed to protect national security. Investing in hiring for aptitude and training in key new technologies will address unfilled security roles over time as the hiring and training pipeline matures. This deliberate investment in the American workforce will also provide a vital conduit for providing economy-stimulating new skilled job opportunities for U.S. workers.

**Government actions that could help address these challenges**

There are several actions the federal government can take to begin addressing these challenges.

As we all know, NIST[17] does a great job with FIPS and special publications to provide smart guidance on security and other information-handling processes. The EO requires NIST to work to determine the implementation of many directives in collaboration with other agencies such as the Commerce Department. The process to gather relevant input to the proposed rules is on an aggressive time scale, which makes sense due to the urgency of the threats but can lead to implementations with unintended consequences. NIST can help by ensuring concerns with various proposed measures have been investigated in terms of expected impact in exchange for the effort.

In the recent SolarWinds attack, "SolarWinds saw signs of hackers invading their networks as early as January of 2019, about eight months earlier than the previously publicly disclosed timeline for the sweeping cyber-espionage campaign, and nearly two years before anyone discovered the breach.[18]" The United States must not only focus on breach response due to supply chain or other attacks, but also invest in identifying security vulnerabilities and coordinate fixes across the supply chain ideally before they are exploited. If we invest in response, detection, prevention, we will not be forced to be reactive only.

Many roles are needed at various technical skill levels to ensure comprehensive coverage of necessary security functions. Most of the requests for additional budget for cybersecurity focus on breach detection and incident response, rather than prevention activities and proactive vulnerability remediation via VDPs. While an "assume breach" security posture is recommended, focusing mostly on the post-breach actions leaves under investments in greater ROI preventative security activities.

16 https://www.lutasecurity.com/post/luta-security-highlights-for-zoom-bug-bounty-programs

17 https://www.nist.gov/

18 https://www.cyberscoop.com/SolarWinds-ceo-reveals-much-earlier-hack-timeline-regrets-company-blaming-intern/

Efforts supporting detection and response to breaches and vulnerabilities are shared resources inside an organization that are currently overstretched and covering numerous government directives at once.

These resources are overstretched even further due to the requirement for all civilian agencies to launch a Vulnerability Disclosure Program (VDP) to comply with CISA's Binding Operational Directive (BOD) 20-01[19]. The same internal personnel resources for VDPs are often needed to investigate and respond to these ongoing attacks. The federal government could address this overbooking of essential internal security personnel by investing in tools to identify vulnerabilities more frequently themselves, and enough skilled personnel to comprehensively investigate and fix incoming vulnerability reports.

Another important action this Committee and Congress could do is measure the maturity of the vulnerability response efforts of the federal agencies and their contractors now, and on at least an annual basis. Performing a comprehensive federal civilian agency gap analysis and maturity assessment will identify critical gaps in people, process, and technology and also support maturity-based metrics, which will measure improvements in cyber security and cyber resilience. These maturity measures could conceivably be part of the annual Federal Information Security Modernization Act[20] (FISMA) assessments. Since the cybersecurity maturity of any given organization changes over time with increased or decreased investments in tools, automation, and skilled key team members addressing an evolving threat landscape, performing maturity assessments should become part of the fabric of our cyber resilience strategy to deal with individual and supply chain vulnerabilities consistent with ISO standards.

The federal government must direct what resources we have while also growing our capacity at scale. As part of expanding CISA's role and resources, CISA should apply a system dynamics approach that models the effects of changing variables in a complex system, focusing on a targeted approach to enhance security outcomes. Some of these variables include the cybersecurity maturity of different links in the supply chain, the current availability of tools to assist in scaling efforts, and the readiness of a trained workforce able to meet different technical requirements as threats change. What we choose to invest in will change these variables in people, process, and technology, that in turn change the calculus for the entire system. Tools can close some gaps, as long as there are skilled operational workers to run them, and analysts are trained to interpret the results and act upon them strategically.

Since pushing on one lever in the system changes the calculus and behavior of the interconnected parts of the system, we can use a system dynamics approach to help inform ROI analysis over time. This will help the United States anticipate the changing needs in people, process, and technology to meet threats today and tomorrow, rather than the cycle of applying one-size-fits-all measures and chasing the threats of yesterday.

19 https://cyber.dhs.gov/bod/20-01/#fn:18

20 https://www.cisa.gov/federal-information-security-modernization-act

**Strengths and limitations of federal actions protecting against and responding to supply chain attacks**

The recent cybersecurity Executive Order provides requirements to address multiple cybersecurity problems at once, a bold and necessary step to catch up in our paying down of technical debt that has amassed like unread messages in the security inbox of the Internet. There are a few concerns and limitations to the proposed measures, and areas of concern where the devil lies in the details of implementation. Some recommendations in the EO may inadvertently introduce new risks by concentrating sensitive information into an attractive new aggregated target for adversaries if not properly managed.

Additionally, BOD 20-01 provides a welcome and much-needed forcing function to get federal agencies to respond to security vulnerability reports from the public, but resources and expertise to support those programs are often overstretched internally to handle breach investigations as well as first party and supply chain vulnerabilities and attacks.

Finally, there are important initiatives that over time will no doubt enhance the speed of responding to supply chain vulnerabilities and compromises, like the Software Bill of Materials (SBOM), but lack definition and implementation studies at this time. This makes them a premature requirement for the near term, possibly distracting from other efforts that could be implemented yielding a better security ROI in exchange for the effort.

A summary of challenging areas include the Cybersecurity Executive Order and BOD 20-01:

- Executive Order:
  - Centralized breach reporting for incidents under active investigation in progress will create an attractive target for adversaries wanting to know the state of their intrusion campaign efforts as investigations unfold. Determining who gets access to this information will be essential, unless the EO is amended to allow for after-action reporting once remediation and recovery actions are already taken.
  - Mandatory breach disclosure of three days for the most serious incidents might not be possible at that stage in the investigation, because they may not know yet they have a serious breach. Providing an exemption for later discoveries as the investigation unfolds may inadvertently reward organizations with slower investigative processes, while punishing organizations with faster and more sophisticated breach detection and investigation capabilities;
  - The SBOM requirement has yet to be defined and adopted even in some of the largest organizations, and like rolling out Multifactor Authentication (MFA) across the federal government and its suppliers, it will be a huge, industry-wide undertaking. Unlike the ambitious timelines for MFA adoption, SBOM does not have a well-understood model for the people, process, and technology needed for a successful rollout. CISA and NTIA should perform studies to measure the beneficial security outcomes that producing and consuming SBOMs require.

- BOD 20-01:
  - Impacts federal agencies level of preparedness - Since the SolarWinds and Microsoft Exchange investigations have the federal government scrambling to deal with its aftermath, it is unclear what steps, if any, federal agencies have taken to systematically assess their ability to carry out their cyber investigation and response duties on multiple fronts at once.
  - Same personnel, multiple functions - That could easily sow greater confusion, distracting key internal cyber incident first responders and creating patching backlogs that could be exploited by the very adversaries that launched SolarWinds and the Microsoft Exchange attacks.
  - Delayed metrics, increased risk - Leaving assessment of the gaps in people, process, and tools assessment until the metrics reporting deadline as stipulated in the BOD will leave critical areas understaffed and outgunned while our adversaries continue to operate undetected for months if not longer. The required metrics in the BOD do not include cybersecurity workforce statistics. These delayed and missing metrics increase the risk to national security.

As mentioned above, SBOM is a worthy initiative that will ideally improve supply chain remediation and response. At the same time, the inclusion of SBOM in the EO now is of concern due to many unanswered questions not yet resolved in a scalable way. The concept certainly bears merit in a commonsense way - knowing what other software is included in a product can speed the response in a supply chain vulnerability or incident response scenario. However, producing or consuming an SBOM would have no effect in stopping or detecting either the SolarWinds nor the CodeCov supply chain attacks. The public comment period for defining the minimum SBOM requirements will leave even more questions about the level of effort required for each organization attempting to comply with that section of the EO, depending on the depth of information that is determined to comprise the minimum SBOM.

An ingredient list of software alone is not useful to determine risk quickly without additional analysis. Neither is the addition of vulnerability data, which would at a minimum include what known vulnerabilities affected each software ingredient. This is because from a technical standpoint, a bug in a software ingredient may not be exploitable in all products that contain that software ingredient. Exploitability would be determined in what code paths are taken via the product, and what other countermeasures may be in place in the overall product that obviate or mitigate the underlying software supply chain vulnerability.

There are no tools that can produce this enriched vulnerability data that includes vetting actual exploitability at scale. This ends up in the same resource crunch situation relying on skilled cybersecurity workers to make that final determination of risk and act upon it.

"Although mounting security problems in healthcare and their root causes have clarified that SBOMs might solve several problems, implementation has been slow and there are few data available from the published peer-reviewed literature. Complicating this issue is a lack of out-of-the-box solutions and industry-wide standards, such that organizations have developed homegrown proprietary solutions to improve interoperability and security of their systems. As one example, the Mayo Clinic now requires prospective vendors of medical devices to submit a complete description of all components of their products, including software architecture, as part of its procurement process. This is a rare instance of such information being publicly available for a healthcare entity, however.[21]"

The SBOM working group has not addressed these open questions or developed consensus around standard minimum information. Further, the group has had mostly industry participants with huge existing investments in internal specialized security teams - the security and incident responder 1 percent. We have no broad field data on how less mature organizations will fare in this new requirement versus investing in other fundamental security efforts.

With significant effort and investment across the ecosystem, an SBOM will help speed up supply chain security response. Given the current state of maturity of both the SBOM project and the United States' cybersecurity capabilities, timely and actionable information to address supply chain risks using SBOMs would be a costly and enormous effort. An SBOM requiring too little information at a minimum would force additional skilled security analysis in order to determine risk. With limited cybersecurity workers, performing this data enrichment step could displace vital security work that might have a greater ROI towards the desired secure supply chain outcomes. More real-world data is needed to determine the people and skill requirements to facilitate SBOM production and consumption. With this additional study, I believe SBOM will become an invaluable part of managing software and hardware supply chain security.

## Conclusion

I appreciate this Committee's and CISA's leadership on cybersecurity and supply chain issues. The urgency of action must be balanced with an analysis of the right action at the right time. I believe that the system dynamics approach to assessing relative ROI of various efforts to improve supply chain security is the "work smarter" approach to paying down our accumulated technical debt that contributes to our national security.

In the private sector, among those defending against becoming the vector for the next supply chain attack, investment in internal resource segmentation, access controls, and build integrity processes would have helped prevent or detect SolarWinds and CodeCov at the source of the compromises. Those efforts have industry-proven risk reduction, whereas forward-thinking measures like SBOM hold great promise, but are not yet proven in reducing supply chain attacks.

21 https://www.nature.com/articles/s41746-021-00403-w

What we really need to pay down the technical debt in securing the software supply chain is an understanding of our gaps in people, process, technology to effectively enhance our software supply chain to be resilient and secure. By amending FISMA to measure our maturity and capabilities, now and on an annual basis, we can more efficiently allocate resources, investments, and improve agencies' preparedness for attacks.

We can take on bold new initiatives, such as those outlined in the EO and other regulations, to start making significant improvements in supply chain security and our national cyber resilience. Our success in these security programs depends on our focus on high ROI activities.

Overlapping internal security roles are currently overstretched in both the federal government and contractors, in keeping with the entire industry's cyber workforce shortage. Supporting multiple new and existing security initiatives will require new recruitment, training, and funding for additional personnel and tools to meet current and future supply chain threats.

Thank you for this opportunity to testify before the Committee today on this critical issue.

I look forward to answering any questions you may have for me.