Department of Justice

STATEMENT OF

TONYA UGORETZ
ACTING ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"UNDERSTANDING AND RESPONDING TO THE SOLAR WINDS SUPPLY CHAIN ATTACK: THE FEDERAL PERSPECTIVE"

PRESENTED
MARCH 18, 2021

STATEMENT OF
TONYA UGORETZ
ACTING ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"UNDERSTANDING AND RESPONDING TO THE SOLAR WINDS SUPPLY CHAIN ATTACK: THE FEDERAL PERSPECTIVE"

PRESENTED
MARCH 18, 2021

Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the invitation to provide remarks on the FBI's role in the Cyber Unified Coordination Group ("UCG") in relation to the recent SolarWinds intrusion.

The SolarWinds incident is the latest in a long line of malicious cyber activity that threatens the health and safety of the American people, and the national and economic security of our country. The individuals who conduct cyber intrusions, and the officials who direct or condone them, believe they can compromise United States networks, steal our financial and intellectual property, and hold our critical infrastructure at risk, all without incurring risk themselves.

The FBI sits at the convergence of United States Government efforts to change this risk calculus. As a member of both the law enforcement and intelligence communities, with domestic and international reach, the FBI is focusing our unique authorities, and our ability to engage with international law enforcement, domestic victims, and key technology service providers, to illuminate how foreign actors are using global infrastructure to compromise United States networks.

We do this not just to understand the malicious activity but also, by enabling the actions of our public and private partners as well as our own, to disrupt it and impose a cost. Our cyber strategy, announced by Director Wray in September, is focused on imposing risk and consequences on cyber adversaries — whether they are acting to benefit criminal enterprises or foreign powers.

Key to our strategy is using the information and insight we develop through our investigations to support our full range of public and private sector partners who defend networks, build international partnerships, sanction destabilizing behavior, collect foreign intelligence, and conduct cyber effects operations. Our collective actions to combat cyber threats are most impactful when they are joint, enabled, and sequenced for maximum impact.

The FBI and Cyber Incident Response

In December 2020, the FBI, the Cybersecurity Infrastructure and Security Agency ("CISA"), and the Office of the Director of National Intelligence ("ODNI"), with support from NSA, formed a Cyber Unified Coordination Group ("UCG") to coordinate the response to the SolarWinds incident, as provided for in Presidential Policy Directive ("PPD") 41. PPD-41's principles guiding the Federal response to a significant cyber incident include balancing national security and investigative requirements, which the FBI leads through a line of effort called Threat Response, and restoration and recovery, which CISA leads through a line of effort called Asset Response. These are complementary efforts in which our responders coordinate engagement with victims. And the information we learn through our investigation identifies new victims and indicators that help inform CISA's response, and vice versa.

The FBI's approach to Threat Response is informed by our joint law enforcement and intelligence mission. We know the adversary's goal is not just to compromise a network; it is to use that compromise in furtherance of a larger objective. That means we need to not only understand what happened to each victim but also tie together the larger picture by integrating what we learn in our investigation with available intelligence on adversary plans, intentions, and activities, as well as information from our prior and ongoing investigations. And then, we translate that understanding into action against the adversary.

In this investigation, we are using all the tools at the FBI's disposal to identify the following: first, those who have suffered an intrusion, and those who may be targeted next; second, who conducted the activity and how; and third, opportunities to pursue, disrupt, and hold accountable those responsible.

Our work has shown that of the more than 16,000 affected public and private sector customers of the SolarWinds Orion product, a much smaller number have been compromised by follow-on activity on their systems. We have so far identified nine federal agencies that fall into this category, and fewer than 100 non-government entities. We continue to investigate, and information we learn through legal process or voluntary disclosure may change this assessment.

The FBI, our fellow Intelligence Community agencies, and CISA have seen and warned of China's and Russia's efforts to inject malicious code into software programs, undermining our trust not only in the programs we all rely on but also in the automated updates that are supposed to increase our security, not compromise it.

Russia conducted the most damaging cyber attack in history, NotPetya, by inserting malicious code into a seemingly routine update for Ukrainian accounting software, starting a global chain of events that crippled shipping companies, pharmaceutical manufacturers, and hospitals. The Russian government hackers responsible for that and many other destructive attacks were indicted in October 2020.

Last July, we issued an alert that the software China's Tax Bureau mandates that United States companies use in order to operate within China's market contained malware that installed a hidden backdoor to the networks of organizations using the software. At least two Western companies operating in China detected malware that was delivered through Chinese vendors that were responsible for releasing upgrades to the software.

We have also seen intrusions by both nation states and cyber criminals into Managed Service Providers, where, by infecting one system, they can access the networks of hundreds of potential victims.

The SolarWinds intrusion takes all of this to yet another, more dangerous level. By purposely infecting a product widely used by enterprises to manage their networks, the adversary gained widespread access and visibility, and executed their plan with a degree of sophistication, tradecraft, and thoroughness that made it extremely difficult to detect.

For the FBI this has been a national response, managed by the FBI's Cyber Division, whose personnel I am honored to lead. Our agents have been in direct contact with victims and with private industry partners with evidence that has helped us identify who is compromised and who is vulnerable. Our technically trained incident response assets throughout the country, collectively known as our Cyber Action Team ("CAT"), have assisted affected entities. Our field offices with experience in complex national security cyber investigations are our hubs for triaging the data we acquire through legal process, from partners, and through other lawful means. And our digital forensics and intelligence personnel are exploiting that information for indicators and intelligence that will help us to attribute the activity to those responsible, and to disrupt them and cause them pain.

Conclusion

The SolarWinds incident shows the investments in time, money, and talent our adversaries are willing to make to conduct malicious cyber activity against us, and the importance of shifting their risk calculus to make all this effort <u>not</u> worth their while. It drives home what we already know—that only a whole-of-society approach will be effective against these threats.

In that vein, we truly appreciate the proactive cooperation of the private sector in this incident. It has made a difference in the UCG's ability to investigate it, mitigate it, and learn from it. It has also highlighted how vital private sector cooperation is to our broader work protecting America from cyber threats. The virtuous cycle we can drive when we work together

has been on display in the SolarWinds response: information from the private sector fuels our investigations, allows us to identify evidence and adversary infrastructure, and enables us to hand off leads to intelligence and law enforcement partners here and abroad. Our partners then put that information to work and hand us back more than we started with, which we can then use to arm the private sector to harden itself against the threat. By leaning into our partnerships, all of us who are combating malicious cyber activity become stronger while we weaken the perpetrators together.

Another aspect of our work with the private sector that this incident has highlighted is the importance of speed. Information about an intrusion is a lot more helpful the day it is discovered than it will be months later. Quick action from the private sector in this incident was an enormous public service, but the fact is, we are not always so fortunate in the speed with which we obtain the evidence we need. The FBI uses the full range of its authorities, including the Foreign Intelligence Surveillance Act, human sources, and other national security tools as well as criminal legal process, to learn how foreign adversaries are using U.S. infrastructure to target victims. We and every other part of the United States Government that operates inside the United States uphold the Constitution and our laws, which require specificity, and often probable cause and prior court authorization, before we issue compulsory process. So there is no substitute for quick, voluntary action by private owners of U.S. networks and infrastructure when we seek to act quickly against a threat.

The FBI, with our fellow UCG members, will continue taking every necessary action to investigate this incident, identify and hold accountable those responsible, and share information with our partners and the American people. We are focused not only on how we will confront the unique challenges we face in cyberspace, but also why we pursue our cyber mission: so the American people can have safety, security, and confidence in our digitally connected world.

Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.