March 18, 2021

Testimony of the Federal Chief Information Security Officer

Christopher J. DeRusha

United States Senate

Homeland Security and Governmental Affairs

Hearing on

Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify today on the Office of Management and Budget's (OMB) role in setting the Federal cybersecurity agenda, including our response to the SolarWinds supply chain compromise. Today, I will discuss the Federal response and the actions that we are taking to mitigate future sophisticated cyber-attacks targeting the Federal Government.

As the Federal Chief Information Security Officer, I am responsible for developing the Federal cybersecurity strategy and overseeing its implementation to protect Federal information systems and data, and improve the overall cybersecurity posture of the United States on behalf of the Federal CIO and OMB Director. Our team at OMB is responsible for partnering with agencies to ensure that their cybersecurity activities are aligned to Administration priorities, and that the Federal budget provides the necessary resources for them to be successful.

Current Status of the SolarWinds Response

We are at a crossroads for the nation's cybersecurity. The SolarWinds incident exposed gaps in our cybersecurity capabilities and risk management programs, not just in the Federal government, but in some of the most mature and well-resourced companies in the world. This event should serve as both a wakeup call and a galvanizing opportunity for the Federal Government and industry to come together and tackle these threats with renewed resolve. This collaboration is critical, as private-sector entities have primary responsibility for the defense and security of their networks. The government must communicate threat assessments to inform private-sector security operations and ensure common situational awareness.

This incident comes amid a series of aggressive and high-profile attacks on Federal systems, attempted theft of the data used to develop the COVID-19 vaccines, ransomware attacks on U.S. hospitals, and new technology and security challenges that arose with the rapid shift to remote work. These myriad challenges underscore the importance and urgency of modernizing Federal IT and strengthening U.S. cybersecurity capabilities.

OMB plays an indispensable role in responding to these threats. Immediately after agencies detected the SolarWinds incident, OMB began coordinating with the Cyber Unified Coordination Group (UCG), which is leading a national response to the incident and ensuring the security of the Federal civilian enterprise. I would like to acknowledge our partners, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council (NSC), the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), the National Security Agency (NSA), and others who are leading efforts to better understand the impact and recovery needs from this significant cybersecurity incident.

In coordination with the UCG, OMB continues to work with agency executives to collect data on the impact of the SolarWinds supply chain compromise, and to identify capability and resourcing gaps in affected agency response and recovery efforts. My office continues to leverage its partnerships with Chief Information Officers and Chief Information Security Officers, leading regular Council meetings where we identify common challenges, share best practices, and coordinate a consistent approach to cybersecurity across government.

Active Cybersecurity Initiatives

We have many activities already under way that will enhance our long-term cybersecurity defense. Today, I will highlight five efforts in particular:

1) Aligning agency budgets to the White House cybersecurity agenda and Federal statutes;
2) Working with CISA to understand the threat we face and gaps in cybersecurity seen across the interagency, while building a strategy for moving the Federal Government forward and bolstering our protections;
3) Leveraging the Technology Modernization Fund to invest in modernizing our aging IT infrastructure and strengthening cybersecurity defenses;
4) Using the authorities of the Federal Acquisition Security Council to identify and address supply chain risks in our environment; and
5) Transitioning to Zero Trust Architecture.

Aligning Agency Budgets and Working with CISA

The SolarWinds compromise followed decades of underinvestment in Federal IT. We must act with urgency to protect against future cybersecurity attacks, but to do so will take significant resources. Not only do agency CIOs and CISOs know the challenges we face with legacy IT, the impacts have been felt broadly to the point that now it has become a roadblock to delivering on agency missions in service of the American people. This Administration is committed to investing in the infrastructure, systems, and people needed to build back better Federal IT, confirming that it securely meets the needs of the American public. The American Rescue Plan laid the foundation for a renewed investment in cybersecurity and includes an additional $650 million in funding for CISA to provide enhanced monitoring of Federal networks and response activities when incidents occur. This investment will accelerate a shared delivery model for cybersecurity services, expertise, and risk-sharing. This funding will bridge the gap in areas such as endpoint detection, cloud security, and security operation centers.

At OMB, we are working diligently to identify the budgetary needs of agencies in response to the SolarWinds incident. Future budget requests will be aligned to prioritize the immediate response to this incident and to identify opportunities to harden our IT infrastructure against future attacks. Security is expensive when done properly, but it is even more costly when it is neglected. Incident and breach recovery are costly, not only financially but in reputation, trust, and perception.

Technology Modernization Fund

One of the innovative funding tools at our disposal is the Technology Modernization Fund (TMF). To date, this centralized account has made initial project awards of nearly $126 million in priority modernization projects, while providing transparency and accountability in achieving successful outcomes. The American Rescue Plan provides $1 billion for the TMF and expands our opportunities to resolve the cybersecurity challenges posed by aging Federal IT systems. I look forward to working with the TMF Board so that future modernization efforts prioritize cybersecurity as an area of government-wide impact.

Federal Acquisition Security Council

In my role as Federal CISO, I also chair the Federal Acquisition Security Council (FASC). This body is responsible for coordinating a whole-of-government effort to identify and address risks to the Federal government's information and communications technology supply chain. We are an interagency council responsible for carrying out four responsibilities:

- Identifying, and recommending to the National Institute of Standards Technology (NIST) the development of supply chain risk management (SCRM) standards, guidelines, and best practices to increase consistency among agencies' SCRM programs;
- Developing criteria for sharing risk information across the USG and private sector;
- Coordinating government-wide efforts to mitigate risk to the Federal government's information and communications technology (ICT) supply chain; and
- Evaluating whether an information technology poses sufficient risk to the Federal Government to warrant exclusion from Federal procurements and/or removal from Federal information systems.

Zero Trust Architecture

Finally, I want to highlight OMB's role in leading agencies to transition to a "Zero Trust" paradigm. Zero Trust is an evolution in cybersecurity that moves away from the historic approach of protecting the network perimeter. Instead, as the frequency and sophistication of attacks increase, a Zero Trust approach assumes that a network may be compromised at any time, and adversaries may already be present in the environment. In this model, real-time authentication mechanisms constantly "test" users, block suspicious activity, and prevent adversaries from the kind of privilege escalation that they used in the SolarWinds compromise.

This approach relies on a strong foundation of identity, credential, and access management capabilities along with a shift to continuous monitoring and dynamic management approaches. A shift to Zero Trust does not represent a new form of technology, nor is it a journey that IT professionals can take alone. Many of the tools we need already exist within industry and agency environments, but implementing a Zero Trust approach is a shift in mindset that requires commitment and focus from all levels of an organization. This includes educating the workforce, engaging with business owners to assess impacts on mission delivery, and obtaining buy-in from senior leadership to sustain financial investments and culture change over time.

Future Areas of Focus

These activities are essential for improving Federal cybersecurity, but they are not sufficient. To maintain our defense in the long run, we must also strengthen the partnership between Congress and Federal agencies to direct resources where they are most needed to fund agency detection, prevention, and recovery efforts. It is also critical to support cybersecurity research and development to enable new tools for securing cyberspace. The cybersecurity funding in the American Rescue Plan is just a down payment. We have years of technical debt to pay off, and the pace of modernization is accelerating.

In addition to funding cybersecurity, we must also invest in our Federal workforce. We need a team of professionals who can support, manage, and identify risks in new technologies across the Federal government. To keep pace with modern technological change, they must be able to hire a modern workforce – one with critical IT and cybersecurity qualifications. Today, Federal agencies struggle to attract competitive talent, keep pace with private-sector pay, and hire quickly enough to replace departing employees.

This Administration is focused on continuing the use of reskilling and upskilling training programs to fill the gap by reinvesting in existing employees. We will leverage the National Initiative for Cybersecurity Education to expand our efforts on cybersecurity education, training, and workforce development. We will also expand the government's cadre of digital services and technology experts at the U.S. Digital Service and GSA's Technology Transformation Service – two groups with a proven record of combining cutting-edge technology skills, an innovative approach to service delivery, and a deep understanding of the Federal Government's mission. Finally, we will continue to rely on the Scholarship for Service CyberCorps program to bring promising cybersecurity talent into the Federal Government at the start of their careers. In a world of constantly evolving technology and expanding cybersecurity threats, the Government must bring together the brightest talent to tackle our most complex challenges.

Conclusion

As illustrated by the SolarWinds incident, the cyber risk landscape is continuously evolving, as are our adversaries along with it. The introduction of new technologies and the advancement of adversaries' tactics, techniques, and procedures mean that cybersecurity is an ever-changing field, and the Nation's approach to cybersecurity must be dynamic. The Federal Government and the Nation can overcome these challenges but it will take sustained effort, meaningful long-term investment, and a constant agility to assess effectiveness of our efforts and adapt to new threats. I commit to continuing to bring agencies together in a coordinated approach to become more resilient and prepared for future challenges. I look forward to working with Congress on updates to legislative authorities, securing the necessary funding for IT modernization, and building on these lessons learned to continue to drive innovation, making the Federal government a leader in cybersecurity.