June 12, 2024

Re: Reducing Federal Cybersecurity Risk Following the Cyber Safety Review Board's *Review of the Summer 2023 Microsoft Exchange Online Intrusion*

Dear Executive Branch Leaders:[1]

On April 2, 2024, the U.S. Government released the Cyber Safety Review Board's (CSRB) review of a cyber attack on Microsoft-hosted cloud environment that resulted in major public and private sector compromises. These lessons should inform a resilient security posture in an era of geopolitical tension and increased targeting from malicious actors.

However, the CSRB, as an advisory body, can only go so far to address the underlying threat that poor security poses to the U.S. government and national security. To improve the security and resiliency of the United States, the federal government must take steps to increase vendor diversity and ensure products with poor security are no longer acceptable within federal government networks.

At its core, the CSRB report showed that the existing, dated approach to security — often with a legacy vendor — creates devastating, preventable errors and serious breaches. Major platform providers — particularly those serving public sector and critical infrastructure organizations — have a heightened responsibility to advance the best security practices.

Many see a software concentration risk among public-sector organizations around the world stemming from the use of the same vendor for operating systems, email, office software, and security tooling. This approach raises the risk of a single breach undermining an entire technology ecosystem. Recognizing this, Senators Eric Schmitt (R-MO) and Ron Wyden (D-OR)

[1] Please refer to pages 4-8 for a complete distribution list.

have called on agencies to "embrace an alternate approach, expanding [the] use of open source software and software from other vendors, that reduces risk-concentration."

As the 2021 Executive Order on Promoting Competition in the American Economy notes, "Agencies can and should further the policies set forth in section 1 of this order by… adopting pro-competitive regulations and approaches to procurement and spending." Competition cannot exist without accountability. We therefore stand with the Senators, the White House, and the Cybersecurity and Infrastructure Security Agency (CISA) in their efforts to improve resiliency, ensure strong security baselines for software products, and encourage competition in the marketplace for these services. As the National Cybersecurity Strategy states, "responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes." Doing so will help to "drive the market to produce safer products and services while preserving innovation and the ability of startups and other small- and medium-sized businesses to compete against market leaders." We agree. A multi-vendor approach to the security of government networks advances both of these goals, and would help to ensure that products with poor security are no longer acceptable within federal government systems.

We urge you to consider actions that can be taken at the agency level to protect your networks and systems and transition your agency to a secure by design approach.

1. **Assess your software concentration risk.**

   A comprehensive assessment of the agency's software supply chain is crucial to identify and mitigate software concentration risks. Over-reliance on a limited number of vendors or specific software components creates a risk to resilience to vulnerabilities and disruptions, cyberattacks, and potential exploitation. A thorough analysis should evaluate the agency's entire software ecosystem, including critical systems and applications, to determine the extent of software concentration risk. This assessment should inform strategies to diversify suppliers, develop redundant capabilities, and establish robust security measures to ensure the resilience and security of your software systems.

2. **Review past security performance in your procurement process.**

   To maintain a robust security posture in an ever-changing threat landscape, it's essential to have the flexibility to evolve your procurement strategies. This includes regularly evaluating vendor relationships and considering their security performance alongside other factors like delivery and quality. If a vendor's product has been compromised, especially if it has impacted your agency, it's crucial to re-evaluate its suitability for your needs. Resources like CISA's list of top routinely exploited vulnerabilities can be valuable tools in this process, helping you make informed decisions that prioritize the protection of your agency's critical data and systems.

3. **Switch to a multi-vendor environment.**

   Relying on a single vendor for your critical IT is like putting all your eggs in one basket. If that vendor is breached, an entire agency's operations could be compromised. This over-reliance on single vendors is a growing concern, as many public sector organizations worldwide are using the same provider for everything from operating systems to security tools.

   To mitigate this risk, we recommend diversifying the public sector technology ecosystem through a multi-vendor approach: an approach that is increasingly adopted in the private sector, and which fosters competition and innovation among vendors. By developing and adhering to open standards, agencies can ensure interoperability, making it easier to switch out individual products if they become insecure. Diversification of cybersecurity providers has already proven its value, and it's time to adopt this model more broadly across the government.

   If there is a breach, or if a provider fails to protect customer information, organizations and procurement officials should have the option of pivoting quickly. Without this option they are at the mercy of exploited systems. This should include the ability to trigger a security recertification for products suffering major security incidents, as well as considering past security performance in buying decisions.

In today's landscape of constantly evolving threats, the status quo is not sufficient. As members of the global online community, we recognize our role in protecting billions of people against these kinds of threats. We are happy to bring together the following co-signatories to share their thoughts with you, whenever helpful.

Respectfully submitted,

Coalition for Fair Software Licensing (CFSL)
Computer & Communications Industry Association (CCIA)
Internet Infrastructure Coalition (i2C)
NetChoice
Software & Information Industry Association (SIIA)

Distribution List

Addressees:

The Honorable Antony Blinken
Secretary of State
U.S. Department of State

The Honorable Janet Yellen
Secretary of the Treasury
U.S. Department of the Treasury

The Honorable Lloyd Austin III
Secretary of Defense
U.S. Department of Defense

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice

The Honorable Deb Haaland
Secretary of the Interior
U.S. Department of the Interior

The Honorable Thomas Vilsack
Secretary of Agriculture
U.S. Department of Agriculture

The Honorable Gina Raimondo
Secretary of Commerce
U.S. Department of Commerce

The Honorable Julie Su
Acting Secretary of Labor
U.S. Department of Labor

The Honorable Xavier Becerra
Secretary of Health and Human Services
U.S. Department of Health and Human Services

The Honorable Adrianne Todman
Secretary of Housing and Urban Development
U.S. Department of Housing and Urban Development

The Honorable Pete Buttigieg
Secretary of Transportation
U.S. Department of Transportation

The Honorable Jennifer Granholm
Secretary of Energy
U.S. Department of Energy

The Honorable Dr. Miguel Cardona
Secretary of Education
U.S. Department of Education

The Honorable Denis McDonough
Secretary of Veterans Affairs
U.S. Department of Veterans Affairs

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
U.S. Department of Homeland Security

The Honorable Michael Regan
Administrator of the Environmental Protection Agency
U.S. Environmental Protection Agency

The Honorable Avril Haines
Director of National Intelligence
Office of the Director of National Intelligence

The Honorable Isabel Guzman
Administrator
U.S. Small Business Administration

The Honorable Martin O'Malley
Commissioner
Social Security Administration

The Honorable Dr. Sethuraman Panchanathan
Director
National Science Foundation

The Honorable Bill Nelson
Administrator

National Aeronautics and Space Administration

The Honorable Samantha Power
Administrator
U.S. Agency for International Development

The Honorable Carrie Safford
Secretary
U.S. Nuclear Regulatory Commission

The Honorable Rob Shriver
Acting Director
Office of Personnel Management

The Honorable Robin Carnahan
Administrator
General Services Administration

The Honorable Sharon Franklin
Chair
Privacy and Civil Liberties Oversight Board

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

General Timothy D. Haugh
Director
National Security Agency

The Honorable Harry Coker, Jr.
National Cyber Director
Office of the National Cyber Director
The White House

The Honorable Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Tech
National Security Council
The White House

Copies to:

Senator Mark Warner (D-VA)
Chair
Senate Select Committee on Intelligence

Senator Marco Rubio (R-FL)
Vice Chairman
Senate Select Committee on Intelligence

Senator Jack Reed (D-RI)
Chair
Senate Committee on Armed Services

Senator Roger Wicker (R-MS)
Ranking Member
Senate Committee on Armed Services

Senator Gary Peters (D-MI)
Chair
Senate Committee on Homeland Security & Governmental Affairs

Senator Rand Paul (R-KY)
Ranking Member
Senate Committee on Homeland Security & Governmental Affairs

Representative Mike Turner (R-OH)
Chair
House Permanent Select Committee on Intelligence

Representative Jim Himes (D-CT)
Ranking Member
House Permanent Select Committee on Intelligence

Representative Mike Rogers (R-AL)
Chair
House Committee on Armed Services

Representative Adam Smith (D-WA)
Ranking Member
House Committee on Armed Services

Representative Mark Green (R-TN)

Chair
House Homeland Security Committee

Representative Bennie Thompson (D-MS)
Ranking Member
House Homeland Security Committee

Senator Angus S. King Jr. (I-ME)
Former Co-Chair, Cyberspace Solarium Commission

Senator Ron Wyden (D-OR)
Chair
Senate Committee on Finance

Senator Eric S. Schmitt (R-MO)