Memorandum: "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security" and Major Security Risks to Consider

BLUF: Microsoft's continued management of government cloud systems endangers U.S. national security due to its ongoing failures in basic cybersecurity practices, reticence to work with federal agencies to investigate intrusions, and conflicts of interest regarding the Peoples' Republic of China.

Failures in basic cybersecurity practices: When PRC-affiliated hacking group Storm-0558 compromised Microsoft's cloud environment, it accessed and exfiltrated the email accounts of the most senior U.S. government officials managing relationships with the People's Republic of China. Through still-unknown mechanisms, the attackers obtained a virtual skeleton key that should never have existed, allowing access to any Microsoft Exchange Online email account on the cloud. The intrusion's scale, severity, and duration were caused and subsequently worsened through a pattern of several years of avoidable cybersecurity lapses by Microsoft.

Failure to work with agencies to investigate attacks: Although the State Department initially discovered Storm- 0558's intrusions, Microsoft could not or would not provide the logging data needed to conduct a comprehensive investigation because some government agencies had not paid for premium licenses. Microsoft's concealment of basic cybersecurity features behind additional paywalls meant government agencies could not comprehensively view or analyze intrusion activity. After the Commerce Department contacted CISA for assistance, Microsoft submitted an incomplete dataset and limited information about the threat actor's infrastructure, hampering federal investigations for no obvious reason.

Conflicts of interest with the world's worst cyber-offender: According to Microsoft, "Any time Microsoft detects a security threat to Azure, Office 365, or another service running on that cloud platform, every other service on that platform gets the benefit of that knowledge." However, China's 2021 Cybersecurity Law requires enterprises to first report all cyber incidents and vulnerabilities to the CCP before other actors or the public, creating a one-way intelligence flow that privileges China over the United States. While Microsoft asserts it did not follow this law in this case, it admits that spikes in Chinese cyber violations "coincide with the first full year of China's vulnerability disclosure requirements." During the Storm-0558 investigation, Microsoft sent an email with sensitive victim and investigative details about the intrusion directly to the People's Republic of China and gave several incorrect or misleading public statements that downplayed or obfuscated the radius, scope, and impact of the intrusions. Despite pressure from federal agencies, Microsoft left these and other false statements uncorrected for more than six months and continues to work with the PRC.

Recommendations:

1. Strengthen the U.S. government's multi-cloud capacity to more easily transition between cloud service providers.
2. Establish a proprietary sovereign cloud that increases interoperability between agencies and reduces interoperability between the U.S. government cloud and foreign, commercial, and adversary cloud networks.
3. Update the Federal Risk Authorization Management Program and Department of Defense (DoD) Cloud Computing Security Requirements Guide to:
   a. Ensure that consumer key-signed tokens cannot be used to access sensitive government cloud systems.
   b. Establish a regulatory obligation for cloud service providers to immediately report incidents and vulnerabilities within government cloud infrastructure to the U.S. federal government.
   c. Strengthen notification and support protocols to ensure rapid communication with victims and investigative agencies after cybersecurity incidents.
   d. Mandate enhanced logging, security, and compliance capabilities for all government cloud systems, not just premium subscribers.