May 19, 2026

VIA U.S. MAIL AND ELECTRONIC DELIVERY

The Honorable William M. Blier
Acting Inspector General
U.S. Department of Justice, Office of the Inspector General
950 Pennsylvania Avenue, NW, Suite 4706
Washington, DC 20530

The Honorable Todd Blanche
Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Colin McDonald
Assistant Attorney General
National Fraud Enforcement Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Brett A. Shumate
Assistant Attorney General, Civil Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Re: Request for Investigation of Microsoft Corporation Concerning (i) Potential False Claims Act Violations Arising from Knowing Misrepresentations of Cybersecurity Risks in Federal Contracts and (ii) Potential Conflicts of Interest and Post-Government Employment Violations by Senior Federal Officials Who Subsequently Joined Microsoft

Dear Acting Inspector General Blier, Deputy Attorney General Blanche, Assistant Attorney General McDonald, and Assistant Attorney General Shumate:

The American Accountability Foundation (AAF) respectfully submits this letter to request that the Department of Justice open a formal investigation into Microsoft Corporation and into the

conduct of certain former senior federal officials who oversaw, regulated, or investigated Microsoft before accepting employment or consulting arrangements with the company.

The publicly documented facts, summarized below and detailed in the accompanying memorandum, describe a pattern that, in our view, warrants careful examination by the Office of the Inspector General, the Civil Division, and the new National Fraud Enforcement Division, each within its respective authority.

We do not, in this letter, allege that any individual violated any specific law or regulation. We do believe however, that the cumulative public record raises questions that have not been answered, that the questions are serious, and that the public has a substantial interest in seeing them addressed by the institutions with the authority and the duty to do so.

I. Microsoft's Conduct Surrounding the SolarWinds, Hafnium, Kaseya, Storm-0558, and Midnight Blizzard Intrusions

Between 2019 and 2023, Microsoft suffered five major cyber intrusions perpetrated by Russian intelligence services, Chinese state-sponsored actors, and Russian cybercriminal groups. Taken together, the intrusions were among the most damaging series of breaches of U.S. government information systems in American history. Those intrusions penetrated the National Nuclear Security Administration and the Departments of Treasury, State, Commerce, and Justice, as well as the National Security Council and numerous other federal agencies. They resulted in the theft of tens of thousands of government emails, including correspondence from the U.S. Ambassador to China, the Secretary of Commerce, and senior Microsoft executives themselves.

Of particular concern, public reporting indicates that beginning in 2016, Microsoft had been internally and repeatedly warned of the “Golden SAML” flaw in its Active Directory Federation Services that was ultimately exploited in the SolarWinds compromise. According to those accounts, a Microsoft security architect, Andrew Harris, repeatedly raised the vulnerability to colleagues and supervisors, and was told that addressing it could jeopardize the company's pursuit of a multibillion-dollar federal cloud contract. The flaw was not patched. It was later exploited by Russian intelligence (APT29/Cozy Bear) to penetrate SolarWinds and, through it, federal networks. Microsoft's President Brad Smith later testified to Congress that “there was no vulnerability in any Microsoft product” exploited in the incident, a statement that, on the public record, appears materially at odds with what Microsoft personnel had been told internally.

The Cyber Safety Review Board's March 2024 report on the related Storm-0558 incident separately concluded that Microsoft's security culture was “inadequate" and that the breach was the product of a “cascade of avoidable security failures.”

300 Independence Ave SE
Washington DC 20003
202-495-0720
info@americanaccountabilityfoundation.com

These facts, in our view, present squarely the kind of conduct that the Biden Administration's Civil Cyber-Fraud Initiative was created to address: knowing or reckless misrepresentations by a federal contractor regarding the cybersecurity of products sold to the government. Yet to our knowledge, no False Claims Act investigation of Microsoft's conduct has ever been opened, while other contractors whose conduct appears materially less egregious have been pursued under the same Initiative.

We respectfully request that the Civil Division and the National Fraud Enforcement Division evaluate whether Microsoft's representations to federal customers concerning the security of its Active Directory Federation Services, its Exchange Server products, its authentication systems, and the GCC High cloud platform satisfy the elements of liability under the False Claims Act, 31 U.S.C. §§ 3729 et seq.

II. The FedRAMP Authorization of GCC High and the Subsequent Departure of the DOJ Official Who Pressed for It

A second and related set of facts concerns the FedRAMP authorization of Microsoft's Government Community Cloud High ("GCC High") platform, which is now relied upon by federal agencies to handle some of the government's most sensitive unclassified data.

Public reporting indicates that, in early 2020, Melinda Rogers, then serving as Deputy Chief Information Officer of the Department of Justice, authorized GCC High for DOJ deployment before FedRAMP's review was complete and notwithstanding the inability of independent assessors to obtain basic encryption documentation. Two independent assessors reportedly told FedRAMP it was "difficult to impossible" to properly evaluate the product. The GSA executive director responsible for the program is reported to have said that Ms. Rogers was "not willing to put heat to Microsoft" and that DOJ was "too sympathetic to Microsoft's claims."

In May 2025, Ms. Rogers joined Microsoft.

We do not assume any improper motive on Ms. Rogers's part. We do believe, however, that the Office of the Inspector General is uniquely positioned to determine whether Ms. Rogers complied at all relevant times with 18 U.S.C. § 208 (acts affecting a personal financial interest), 18 U.S.C. § 207 (post-employment restrictions), and the executive-branch standards of ethical conduct at 5 C.F.R. Part 2635 – and, in particular, whether any employment discussions or negotiations occurred during the period in which she was exercising official authority over Microsoft's authorization.

III. The Departure of the Deputy Attorney General and Other Senior Officials to Microsoft and to Firms Representing Microsoft

300 Independence Ave SE
Washington DC 20003
202-495-0720
info@americanaccountabilityfoundation.com

The third set of facts concerns a broader pattern of senior federal officials, including officials who served at the Department of Justice or on the Cyber Safety Review Board – which was established by Executive Order 14028 specifically to investigate the SolarWinds and Microsoft Exchange incidents – subsequently joining Microsoft as employees or consultants, or joining firms that represent Microsoft, in close proximity to their official actions concerning the company. We summarize the principal facts as they appear in the public record:

- Lisa Monaco served as Deputy Attorney General from April 2021 through January 2025. In October 2021, she announced the Civil Cyber-Fraud Initiative, which was designed to use the False Claims Act against contractors who knowingly misrepresent cybersecurity risks. During her tenure, the Department brought such actions against companies whose conduct, on the public record, appears far less serious than the conduct attributed to Microsoft in the same period, including against a medical contractor, a defense contractor, a telecommunications provider, and a university. No such action was ever brought against Microsoft. In May 2025, approximately four months after leaving the Department, Ms. Monaco joined Microsoft as President of Global Affairs.

- John P. Carlin, who served as Principal Associate Deputy Attorney General under Ms. Monaco, was an inaugural member of the Cyber Safety Review Board. He departed the Department in October 2022 for Paul, Weiss, Rifkind, Wharton & Garrison LLP, where he chairs the firm's Cybersecurity & Data Protection and National Security Practice Groups. His firm biography references representation of an unnamed “Fortune 10 Company” in a regulatory matter involving “a complex data security incident involving a third-party service provider,” a description that, on its face, is consistent with Microsoft. In February 2024, Mr. Carlin co-authored an amicus brief in SEC v. SolarWinds Corp. that, in our view, directly contradicts the enforcement theory underlying the Civil Cyber-Fraud Initiative that his former superior had announced.

- Bryan A. Vorndran served as the FBI's representative on the Cyber Safety Review Board. The public record indicates that he was recused from the Board's investigation of the Microsoft Storm-0558 incident and replaced by a colleague. The reason for the recusal has not been publicly disclosed. In June 2025, Mr. Vorndran joined Microsoft as Deputy Chief Information Security Officer.

- Jerry L. Davis joined the Cyber Safety Review Board in November 2022 and, on the public record, fully participated in the Board's investigation of the Storm-0558 incident, which culminated in the March 2024 report concluding that Microsoft's security culture was “inadequate.” Mr. Davis joined Microsoft as a Chief Security Advisor approximately three months later, in June 2024.

300 Independence Ave SE
Washington DC 20003
202-495-0720
info@americanaccountabilityfoundation.com

- Robert E. Joyce served as Director of Cybersecurity at the National Security Agency and as an inaugural member of the Cyber Safety Review Board. After leaving NSA in 2024, he founded Joyce Cyber LLC, which publicly identifies Microsoft among its clients.

- Kemba Walden served as an Assistant General Counsel of Microsoft's Digital Crimes Unit and was an inaugural member of the Cyber Safety Review Board. She departed Microsoft in May 2022 to serve as Principal Deputy National Cyber Director in the Executive Office of the President. She was a signatory to the same February 2024 amicus brief described above.

Federal ethics rules prohibit government officials from participating personally and substantially in particular matters in which they have a financial interest, and they impose cooling-off restrictions on certain officials seeking to represent private parties before their former agencies. Whether each of the individuals named above complied in full with those rules -- and, more importantly, whether the prospect of future employment had any influence on the decisions any of them made while in government -- are questions that the public record cannot answer and that we believe the Office of the Inspector General is best positioned to address.

IV. Requested Action

We respectfully request the following:

- That the Office of the Inspector General open a review of the conduct of the former and current Department of Justice officials identified above -- including Ms. Monaco, Mr. Carlin, and Ms. Rogers -- to determine whether each complied at all relevant times with 18 U.S.C. §§ 207 and 208, the executive-branch standards of ethical conduct, and any applicable recusal obligations, and to determine when employment or representational discussions between those officials and Microsoft (or firms representing Microsoft) began.

- That the Office of the Inspector General coordinate, as appropriate, with the Inspectors General of the Department of Homeland Security, the Federal Bureau of Investigation, and the National Security Agency with respect to the conduct of officials within those components -- including Mr. Vorndran, Mr. Davis, and Mr. Joyce -- who served on the Cyber Safety Review Board and subsequently entered into employment or consulting arrangements with Microsoft.

- That the Civil Division and the National Fraud Enforcement Division evaluate whether Microsoft's representations to federal customers concerning the security of its products and services -- including but not limited to its Active Directory Federation Services, Exchange Server, authentication systems, and GCC High platform -- give rise to liability under the False Claims Act, 31 U.S.C. §§ 3729 et seq.

300 Independence Ave SE
Washington DC 20003
202-495-0720
info@americanaccountabilityfoundation.com

- That the Department evaluate, in coordination with the General Services Administration and FedRAMP, whether the circumstances surrounding the authorization of GCC High warrant any additional review of the FedRAMP authorization process as applied to Microsoft.

V. Conclusion

Public confidence in federal cybersecurity, in federal contracting, and in the impartial administration of federal law enforcement depends on the willingness of the institutions named in this letter to ask hard questions when the public record suggests they should be asked. The facts summarized above and detailed in the accompanying memorandum do not, by themselves, answer those questions. They do, in our judgment, require that they be asked.

We would welcome the opportunity to provide any further information, materials, or assistance that may be useful to the Department's review. Please direct any correspondence to the undersigned at the address above.

Respectfully submitted,
Thomas Jones

Founder and President

Enclosure: Memorandum, *Microsoft Cybersecurity and Post-Government Employment Timeline* (May 14, 2026).

cc: Chair and Ranking Member, Senate Judiciary Committee; Chair and Ranking Member, House Committee on Oversight and Accountability; Comptroller General of the United States

300 Independence Ave SE
Washington DC 20003
202-495-0720
info@americanaccountabilityfoundation.com

Microsoft Cybersecurity and Post-Government Employment Timeline

Overview

Between 2019 and 2023, Microsoft suffered five major cyberattacks, perpetrated by Russian intelligence, Chinese state hackers, and Russian cybercriminals that collectively represent the most sustained and damaging series of breaches of U.S. government systems in American history.

The attacks exploited vulnerabilities that Microsoft had known about, in some cases for years, but declined to fix or even disclose as it sought billions in new federal contracts. They penetrated the National Nuclear Security Administration, the Treasury, State, Commerce, and Justice Departments, the NSC, and dozens of other federal agencies.

They resulted in the theft of tens of thousands of government emails, including correspondence from the U.S. Ambassador to China, the Commerce Secretary, and senior Microsoft executives themselves. A subsequent federal review concluded that Microsoft's security failures were "avoidable" and stemmed from a corporate culture that deprioritized security in favor of revenue and market share.

The attacks triggered an unprecedented government response. President Biden signed an executive order creating the Cyber Safety Review Board specifically to investigate Microsoft's role in the SolarWinds breach. His Deputy Attorney General, Lisa Monaco, launched a new legal initiative (the Civil Cyber-Fraud Initiative) explicitly designed to hold contractors like Microsoft accountable for knowingly misrepresenting cybersecurity risks.

Congress held hearings. The CSRB ultimately published a scathing report calling Microsoft's security culture "inadequate" and demanding an overhaul. Running in parallel through all of it, the federal government spent years trying, and largely failing, to vet Microsoft's cloud platform for the government's most sensitive data. Independent security assessors told FedRAMP the product was "difficult to impossible" to evaluate. One reviewer called the documentation package "a pile of shit."

FedRAMP ultimately authorized the platform anyway -- not because its questions had been answered, but because Microsoft's product was already deployed across Washington. The authorization came with an unprecedented "buyer beware" warning to federal agencies. A senior cybersecurity official called it "security theater."

What followed was something different. SolarWinds, the most devastating of the cyberattacks was curiously never investigated by the CSRB. Rather than face accountability, Microsoft systematically hired away the very people responsible for investigating and regulating it. The timing raises a question that has never been publicly answered: whether employment discussions between Microsoft and some of the officials began while they were still in government, still overseeing the company's products, or still conducting or supervising investigations into its security failures.

Lisa Monaco, the Deputy Attorney General who had launched the initiative designed to prosecute companies for knowingly misrepresenting cybersecurity risks, never investigated Microsoft, limiting her prosecutions only to companies that were involved in far less egregious cybersecurity violations. Instead, she joined Microsoft in June 2025.

Melinda Rogers, the DOJ official who had pushed FedRAMP to approve Microsoft's cloud platform despite years of unanswered questions about its security and encryption and over the objections of independent assessors, joined Microsoft the same month.

Bryan Vorndran, the FBI's representative on the CSRB -- who was recused from at least one Microsoft investigation (Storm-0558) for undisclosed reasons suggesting a conflict of interest -- joined Microsoft as Deputy CISO the following year. His recusal, now viewed alongside his subsequent hire, raises the obvious question of whether Microsoft was already in contact with him while the investigation was active.

Jerry Davis, another CSRB member who fully participated in the Storm-0558 investigation that condemned Microsoft's security culture joined the company within three months of the report's publication, a timeline so compressed it strains the assumption that no discussions occurred beforehand.

Rob Joyce, the NSA's cybersecurity director, who served on the inaugural CSRB, left government and promptly took on Microsoft as a consulting client.

And John Carlin, the Deputy Attorney General's own #2 at the DOJ, who was himself an inaugural CSRB member, departed for a law firm where it appears he may represent Microsoft, and then filed a federal court brief directly contradicting the enforcement theory his former boss had championed.

Federal ethics rules prohibit government officials from participating in matters in which they have a financial interest, and require cooling-off periods before certain officials may represent private parties before their former agencies. What no investigation has yet examined is whether the prospect of future employment shaped the decisions these officials made while still in government. The pattern documented below does not answer that question. But it does demand that someone ask it.

2016 - Microsoft Security Architect Discovers Critical Flaw in Windows Server Software. Company Ignores Flaw to Avoid Jeopardizing Federal Government Cloud Contract

- In 2016, Microsoft security architect **Andrew Harris** discovers a critical "Golden SAML" flaw in the company's Active Directory Federation Services (AD FS) that allows hackers to masquerade as legitimate users and access cloud environments undetected. Harris repeatedly warns colleagues inside Microsoft, but is ignored.[1]

- According to later accounts by Harris, Microsoft knew its version of this master key was dangerously easy to steal but refused to fix it because doing so would have inconvenienced users and risked losing federal government contracts. A Microsoft product manager specifically tells Harris that fixing the AD FS vulnerability risks alienating the federal government at a moment when Microsoft is competing for one of the largest government cloud contracts in US history. Microsoft CEO Satya Nadella signals internally that the contract is critical, and the flaw is left unpatched.[2] Harris ultimately resigns from Microsoft in frustration after years of ignored warnings about the vulnerability.[3]

DOJ Official Who Approves Microsoft's Federal Cloud Platform Later Joins the Company

- Beginning in 2016 (the same year Harris discovers the Golden SAML flaw) Microsoft also begins pursuing FedRAMP authorization for **GCC High**, a cloud platform designed to handle the government's most sensitive data and worth billions in federal contracts. FedRAMP is the federal government's mandatory cybersecurity gatekeeper for cloud products, and authorization unlocks access to the entire federal market.

- In early 2020, **Melinda Rogers**, the Justice Department's deputy chief information officer, authorizes GCC High for DOJ deployment before FedRAMP's formal review is even complete and despite the company's failure to produce even basic encryption documentation. Two independent assessors privately tell FedRAMP it was "difficult to impossible" to properly vet the product. One Microsoft FedRAMP evaluator says, "the package is a pile of shit."[4]

- Despite the serious concerns from evaluators, Rogers presses FedRAMP to "get this thing over the line." GSA's executive director later tells *ProPublica* that Rogers was "not willing to put heat to Microsoft on this," and that the DOJ "was too sympathetic to Microsoft's claims."[5]

[1] https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
[2] https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
[3] https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
[4] https://www.propublica.org/article/microsoft-cloud-fedramp-cybersecurity-government
[5] https://www.propublica.org/article/microsoft-cloud-fedramp-cybersecurity-government

- In May 2025, Rogers, whose role was central to Microsoft's FedRAMP authorization process, joins Microsoft.[6]

2019-2023 Microsoft Hit With Series of Five Unprecedented Hacks Targeting Federal Government Customers, Others

- ***Solar Winds/AD FS (Cozy Bear):*** In September 2019 as Microsoft is pursuing FedRAMP final approval, the Russian Foreign Intelligence Service (*SVR/APT29/*Cozy Bear) begins infiltrating SolarWinds networks. Once inside the victim's networks, they exploit the Golden SAML flaw in Microsoft's AD FS -- the exact flaw Harris had been warning the company about for three years. The breach penetrates the National Nuclear Security Administration, the National Institutes of Health, Treasury, State, DOJ, and several other federal agencies.[7] The flaw remains undetected by Microsoft for over a year and is only discovered when FireEye, a cybersecurity firm, uncovers it while investigating a separate intrusion into its systems.[8] Microsoft President **Brad Smith** later assures Congress in February 2021, that "there was no vulnerability in any Microsoft product that was exploited," a claim Harris says was false.[9]

- ***Microsoft Exchange Server (Hafnium):*** In January 2021, the Chinese state-sponsored group *Hafnium* exploits four zero-day vulnerabilities in Microsoft Exchange Server, breaching more than 30,000 US organizations and federal agencies.[10] Microsoft confirms the Hafnium exploit internally on January 8, 2021, but doesn't issue a patch until March 2nd, 53 days later.[11]

- ***Kaseya/Windows Defender (REvil):*** In July 2021, Microsoft's systems were breached a third time when the Russian cybercriminal group REvil exploits zero-day vulnerabilities in Kaseya's VSA remote management software -- the largest criminal ransomware attack in history to that point, demanding $70 million in Bitcoin from its victims. REvil's payload specifically drops an outdated, expired version of Microsoft's Windows Defender executable that is known to be vulnerable to DLL side-loading attacks – using Microsoft's own security software as the delivery mechanism for the ransomware.[12]

- ***Microsoft Authentication Tokens (Storm-0558):*** In May 2023, Chinese hackers (Storm-0558) use forged Microsoft authentication tokens to breach 25 different organizations and government agencies including State and Commerce.[13] Microsoft's Vice President for Customer Security & Trust **Tom Burt** meets with the NSC's Anne Neuberger days later on May 19, 2023 according to White House visitor logs.[14] The breach results in the theft of approximately 60,000 State Department emails including from the U.S. Ambassador to China

---

[6] https://www.linkedin.com/in/melindarogers/
[7] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic
[8] https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack
[9] https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers, https://www.linkedin.com/posts/andrewfharris_ive-been-outspoken-a-bit-on-how-bypassing-activity-6745561216145588224-R4mj/
[10] https://www.securitymagazine.com/articles/94781-000-us-organizations-breached-by-cyber-espionage-group-hafnium
[11] https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/
[12] https://www.sophos.com/en-us/blog/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses
[13] https://www.oasis.security/blog/automation-is-key-dhs-report-unveils-lessons-from-the-microsoft-exchange-incident
[14] White House Visitor Logs UIN# U75911

and Commerce Secretary Gina Raimondo.[15] Microsoft does not disclose the hack publicly until three weeks later on July 11, 2023.[16]

- ***Microsoft-Federal Government Email Hack (Midnight Blizzard)****:* In November 2023, the Russian APT29 (Midnight Blizzard) uses password-spraying brute force attacks to compromise a legacy Microsoft test account lacking multi-factor authentication. Hackers access Microsoft senior executive and cybersecurity team emails for 60+ days before detection on January 12 2024. Federal agency email correspondence is also stolen.[17]

Biden Signs Executive Order 14028 Establishing Cybersecurity Safety Review Board to Investigate SolarWinds, Microsoft Exchange Breaches.

- On May 12, 2021, President Biden signs EO 14028, directly in response to the SolarWinds attack and Microsoft Exchange breaches. The order creates the Cyber Safety Review Board (CSRB), the first directive of which is to perform an initial review of the SolarWinds incident, and report to the DHS Secretary within 90 days. The order specifies that CSRB would be established in consultation with the Attorney General and that the DOJ will have a mandatory seat on the board.[18]

- On August 25, 2021, President Biden summons tech CEOs to the White House to discuss the SolarWinds attack and other cybersecurity issues.[19] Microsoft promises $150 million in free cybersecurity upgrades to federal agencies, a pledge dubbed the "White House Offer."[20] The upgrades are designed to lock agencies into paid Microsoft products once the free period ends, capturing billions of taxpayer dollars in new federal revenue. Microsoft's own attorneys raise antitrust concerns, but the DOJ takes no action.[21]

Deputy Attorney General Lisa Monaco Declines to Investigate Microsoft, Then Joins the Company She Never Investigated

- On April 21, 2021, Lisa Monaco is sworn in as the 39th Deputy Attorney General. Cybersecurity threats are declared a top priority of the DOJ.[22]

- On October 6, 2021, Monaco formally announces the DOJ's Civil Cyber-Fraud Initiative, promising to deploy the False Claims Act against government contractors who knowingly misrepresent cybersecurity risks.[23] Microsoft's documented conduct in the SolarWinds flaw from 2016 to 2020 fits the description precisely – the most damaging cyberattack in American history and one that the company knew about but failed to disclose -- but Monaco never opens a case against Microsoft under the Initiative.

---

[15] https://www.trtworld.com/article/15160792
[16] https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/
[17] https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system-closed
[18] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
[19] https://www.cnbc.com/2021/08/25/biden-to-host-tech-finance-and-energy-ceos-for-white-house-cybersecurity-summit.html
[20] https://www.techradar.com/pro/microsoft-accused-of-creating-a-monopoly-on-us-government-systems-through-free-upgrades
[21] https://www.propublica.org/article/microsoft-white-house-offer-cybersecurity-biden-nadella
[22] https://www.justice.gov/dag/bio/deputy-attorney-general-lisa-o-monaco
[23] https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

- On July 13, 2022, The White House releases the National Cybersecurity Strategy's first implementation plan to "leverage the False Claims Act to improve vendor cybersecurity." The plan specifically directs the DOJ to "expand efforts to identify, pursue, and deter knowing failures to comply with cybersecurity requirements in Federal contracts and grants."[24] The DOJ still takes no action against Microsoft.

- Instead, Monaco pursues cases against companies whose conduct was far less egregious: a medical provider that misfiled patient records (Comprehensive Health Services);[25] a defense contractor that misrepresented its compliance with cybersecurity requirements, but where no breach occurred (Aerojet Rocketdyne);[26] a telecom provider that self-reported its failure to satisfy certain cybersecurity requirements (Verizon Business Network Services);[27] and a university for paperwork misrepresentation (Penn State).[28]

- In May 2025, Monaco joins Microsoft just four months after leaving the DOJ as the company's new President of Global Affairs.[29]

Biden's CSRB Established to Investigate Microsoft, Staffed by Microsoft, Board Members Later Employed by or Consult for Microsoft

- On February 3, 2022, the DHS establishes the CSRB. Among the inaugural members are **Kemba Walden**, an Assistant General Counsel of Microsoft's Digital Crimes Unit and **John Carlin**, Lisa Monaco's direct report at DOJ. The board also includes **Bryan Vorndran** with the FBI's cyber division and **Rob Joyce**, the NSA's director of cybersecurity.[30]

- DHS and the White House quietly announce that the CSRB's first investigation will *not* include SolarWinds as Biden's EO explicitly required, but instead Log4j, an open-source vulnerability disclosed in December 2021. In fact, the CSRB never investigates SolarWinds, puzzling cybersecurity experts.[31]

- In May 2022, three months after the CSRB declines to investigate Microsoft's role in SolarWinds, Walden departs Microsoft to become Biden's principal deputy of the newly formed White House Office of the National Cyber Director.[32] After Walden's departure, **Jerry Davis** joins the CSRB board in November 2022.[33]

- In October 2022, Carlin departs the DOJ for **Paul Weiss**, one of Microsoft's top outside law firms, which has been described as the "go to spot for Big Tech to fend off an increasingly proactive Biden Administration on antitrust."[34] Carlin chairs the Cybersecurity & Data

---

[24] https://web.archive.org/web/20230713104529/https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf
[25] https://www.justice.gov/archives/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical
[26] https://www.justice.gov/archives/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity
[27] https://www.justice.gov/archives/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully
[28] https://www.justice.gov/archives/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating
[29] https://www.axios.com/2025/05/30/microsoft-policy-promotes-trump-official
[30] https://www.dhs.gov/archive/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board
[31] https://www.propublica.org/article/cyber-safety-board-never-investigated-solarwinds-breach-microsoft
[32] https://www.govtech.com/workforce/national-cyber-director-chris-inglis-reportedly-stepping-down
[33] https://www.linkedin.com/in/jldavisnasa/details/experience/
[34] https://prospect.org/2023/10/26/2023-10-26-dueling-petitions-doj-big-tech-revolving-door/

Protection Practice and National Security Practice Groups.[35] Carlin's law firm bio discloses that he represents a "*Fortune 10 Company in matters involving long-running regulatory attention on core components of the company's business and data privacy practices and in its response to a regulatory inquiry stemming from a complex data security incident involving a third-party service provider*" a description that fits Microsoft precisely.[36]

- In February 2024, Carlin coauthors an amicus brief defending SolarWinds against the SEC's landmark cybersecurity enforcement action.[37] The brief directly contradicted the very legal theory underlying Monaco's own Civil Cyber Fraud Initiative, which promised to hold contractors accountable for knowingly misrepresenting cybersecurity risks. The brief's signatories included among others former CSRB member Kemba Walden, the Microsoft employee who had sat on the inaugural board.[38] In effect, Monaco's own #2 at DOJ was now arguing in federal court against the enforcement doctrine Monaco herself had championed, on behalf of a coalition that included a sitting Microsoft alumna, while also possibly advising Microsoft at Paul Weiss.

- Moreover, three other CSRB members later join Microsoft as employees or consultants. Rob Joyce leaves the NSA in April 2024 to start **Joyce Cyber**, a cybersecurity company that counts Microsoft among its largest clients.[39] In June 2024, Jerry Davis joins Microsoft as a Chief Security Advisor.[40] Bryan Vorndran joins Microsoft in June 2025, as the company's Deputy CISO.[41]

- Notably, separate media investigations report that when the CSRB released its later 34-page report on the Microsoft Storm-0558 hack in March 2024 concluding that the breach resulted from a "cascade of avoidable security failures," the FBI board member was recused and replaced by a colleague.[42] Appendix C of the final report discloses that **Cynthia Kaiser** was the FBI representative on CSRB during the investigation, suggesting the Vorndran was recused. [43] *ProPublica* was told by DHS that "board members are required to step aside if a review includes 'examinations of their employers' products or those of competitors' or if a board member has 'financial interests relating to matters under consideration.'"[44]

- Vorndran's recusal is significant given that he joined Microsoft a year later and suggests the possibility that Microsoft was in fact discussing employment opportunities with members of the CSRB and DOJ in the midst of government investigations into its cybersecurity failures. Jerry Davis, who joined Microsoft just three months after the Storm-0558 report did not recuse himself from the investigation.[45]

---

[35] https://www.linkedin.com/in/john-p-carlin/, https://finance.yahoo.com/news/microsoft-rethinks-law-firm-relationships-081044028.html
[36] https://www.paulweiss.com/professionals/partners-and-counsel/john-p-carlin
[37] https://www.paulweiss.com/insights/client-news/paul-weiss-files-amicus-brief-on-behalf-of-over-20-former-senior-government-officials-in-landmark-sec-enforcement-action-over-cybersecurity-disclosures
[38] https://www.paulweiss.com/media/yjnfn2kc/23-cv-9518-sec-v-solarwinds-brief-of-amici-curiae-former-government-officials.pdf
[39] https://www.linkedin.com/in/rob-joyce-b43445116/, https://www.joycecyber.com/empty-page
[40] https://www.linkedin.com/in/jldavisnasa/details/experience/
[41] https://www.linkedin.com/in/bryan-vorndran-43b3025/
[42] https://www.propublica.org/article/cyber-safety-board-never-investigated-solarwinds-breach-microsoft
[43] https://www.cisa.gov/sites/default/files/2025-03/CSRBReviewOfTheSummer2023MEOIntrusion508.pdf
[44] https://www.propublica.org/article/cyber-safety-board-never-investigated-solarwinds-breach-microsoft
[45] https://www.linkedin.com/in/jldavisnasa/