

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

NATIONAL TREASURY
EMPLOYEES UNION, *et al.*,
Plaintiffs,

v.

RUSSELL VOUGHT, in his official capacity
as Acting Director of the Consumer Financial
Protection Bureau, *et al.*,
Defendants.

Case No. 25-cv-0381-ABJ

THIRD DECLARATION OF ERIE MEYER

I, Erie Meyer, declare the following under penalty of perjury:

1. I served as the Chief Technologist and Senior Advisor to the Director at the Consumer Financial Protection Bureau from October 2021 until February 7, 2025, when I resigned. Because of my experience in that role, I have expertise regarding the agency's website management, data protocols, contract oversight, and the impact of contract terminations.

Mishandled Data Retention Practices

2. I have reviewed the declaration of Charlie Doe, a Contracting Officer at the CFPB, regarding the mass termination of contracts between February 11, 2025, and February 14, 2025—and the CFPB's effort to finalize those terminations as quickly as possible.

3. The highly irregular actions that the Bureau has taken within the past few days to rush the final termination of virtually all of its contracts across the full range of functions raises serious concerns about data preservation and the Bureau's ability to function at all. Final cancellation of the Bureau's contracts will result in the irretrievable impairment and loss of Bureau data. I am also troubled that the Bureau appears not have taken appropriate steps to ensure compliance with this Court's February 14 Order on data preservation.

4. The information in Charlie Doe's declaration accords with information that I have received from several other current Bureau employees—former colleagues of mine—who are in a

position to know this information. They have expressed grave concern that the Bureau's rush to finalize the termination of the vast majority of the CFPB's contracts risks the imminent loss of essential data and records. I understand that the government, upon the insistence of the plaintiffs in this case that these actions were not in compliance with the Court's February 14 Order, has agreed to temporarily suspend cancellation of contracts through the Court's March 3 hearing, but no further. If the government is not immediately prevented from proceeding with contract terminations efforts thereafter, it will be too late to forestall permanent loss of the Bureau's data.

5. My understanding is that the contracts that the Bureau seeks to fully terminate include—among others—contracts with experts (who have sensitive litigation data), with other litigation contractors, and with companies that store, transmit, and maintain Bureau data. That data is crucial to everything from identifying and assisting victims of consumer fraud and providing them court-ordered relief, to tracking the financial information that is critical to the Bureau's role in helping to stabilize financial markets, to responding to consumer complaints. As I explained in my prior supplemental declaration, if the data possessed or maintained by these vendors is deleted or impaired, that would be a catastrophic loss for the Bureau and seriously impair its ability to carry out its obligations.

6. The rush to finalize the termination of the vast majority of the Bureau's contracts is very likely to cause irretrievable data deletion, and to impair the data and records that are not deleted. It is standard industry practice that following contract terminations, contractors delete any government data, because ordinarily contractors are not permitted to retain that data once they no longer have a contract to perform work that requires it. Particularly in the absence of a data preservation clause in the termination notice, contract termination will almost certainly result in the deletion of data either immediately or after a very short period (typically days or weeks). Even if the final termination modification contained a data preservation clause, this rush to terminate

contracts is still very likely to result in the deletion of data and records the Bureau will be unable to lawfully get back. For example, if the retention period elapses before a functioning, approved government System of Record is available to accept and process that data, if there are not enough contracting officers to oversee that the firms are complying with the retention clauses, if the files are corrupted before a CFPB employee is able to detect and act on that emergency, a band-aid of a retention clause will not fully remediate the harm.

7. In addition, in the absence of continuous maintenance of CFPB databases—contracts that I understand the Bureau is seeking to fully terminate—there is a serious risk that the data they contain will be impaired. Without the benefit of virus scanning and other security software, audit logs to ensure that if data is improperly accessed that there is forensic evidence of that access and any manipulation, a continuity of operations protocol or staffing to address any unexpected outages or failures, or meaningful backups to compare data to for authenticating accuracy of the information, the data is at existential risk.

8. Some contracts also provide support for CFPB-maintained data. Those contracts exist because in those cases, the CFPB does not have the capability to maintain the data on its own. Although the CFPB can manage temporary fixes for a limited period of time, if the contracts are permanently terminated and the CFPB must go without support for months or more while those services are re-procured, data will inevitably be impaired.

9. The data possessed and maintained by CFPB contractors includes the personal information of consumers and employees, as well as sensitive information about financial markets and corporations. In addition to the risk of deletion, the rush to terminate the CFPB's contracts puts this data at serious risk of misuse or access by unauthorized parties.

10. I urge the Court to consider the significant and long-term consequences of data loss that could arise from these contract terminations, especially where no clear measures have been

taken to ensure data retention or retrieval.

Mass Cancellation of Cyber Security Contracts

11. I have reviewed the February 24, 2025 declaration of Adam Martinez, the CFPB's Chief Operating Officer. As previously stated in my earlier declaration, I worked alongside Mr. Martinez for several years and respected him as a colleague. In his declaration, he claimed security monitoring tasks were being performed and operations were being maintained. Unfortunately, based on the following facts, I have reason to believe that claim to be false.

12. In recent days, 32 cybersecurity contracts have been cancelled, as reported on [doge.gov/savings](https://www.doge.gov/savings). Of these, five contracts have been posted in detail on the Federal Procurement Data System (FPDS), with a cancellation date of February 13th. The remaining 27 contracts, however, have not yet been published in detail due to what [doge.gov](https://www.doge.gov) has described as a "lag" in FPDS publications. A chart listing all 32 contracts, the cybersecurity impact of that contract, and the date of cancellation, is attached to this declaration as **Exhibit A**.

13. On February 14th, [doge.gov/savings](https://www.doge.gov/savings) read simply "Receipts coming soon, no later than Valentine's day 🍷"¹ Then starting February 15th, [doge.gov/savings](https://www.doge.gov/savings) read "Receipts coming over the weekend!"² Ultimately, on Tuesday February 17th, [doge.gov/savings](https://www.doge.gov/savings) was populated with content including cancelled contracts, including those back-dated to February 14th.

13. I understand that a court order was issued on February 14th, directing the CFPB to preserve and not impair any data held by the Bureau. I am particularly concerned that the cancellation of the 27 remaining contracts may have occurred *after* the issuance of the order, which raises serious questions about whether the Bureau is taking the steps necessary to ensure compliance with the order.

¹ <https://web.archive.org/web/20250214152452/https://doge.gov/savings>

² <https://web.archive.org/web/20250215213222/https://doge.gov/savings>

14. As of the date of this declaration, it remains unclear when these 27 cancellations occurred, aside from the fact that they must have taken place after February 13th, and were touted on doge.gov no sooner than February 18th. The lack of clarity regarding the cancellation timeline and backdating exacerbates my concerns.

15. The cancelled contracts cover a wide range of critical cybersecurity services, including but not limited to:

- Application security (code vulnerability scanning, penetration testing)
- Centralized management and enforcement of security configurations across IT infrastructure
- Cyber vulnerability tracking/reporting across hardware and software
- Certified Information System Auditor training
- Cybersecurity audit/event log analysis
- Cybersecurity contractors for the Security Authorization Environment
- Email server security and encryption
- Identity and access management (including single sign-on and software)
- IT network, systems, and applications management
- Network/application vulnerability scanning
- Secure equipment disposal
- Virus scanning and cybersecurity for SaaS services
- VPN deployment on employee laptops
- Website and file virus scanning, among others.

16. In light of these abrupt cancellations, I am particularly concerned that bureau data and systems are at serious risk of compromise, or have already been compromised.

17. The revocation of contracts for cybersecurity audit and event log analysis is

particularly concerning, because it could mean that there will be no evidence available if unauthorized users are accessing Bureau systems and data. The CFPB would not be able to tell what happened, and it could compromise ongoing litigation, trade secrets, and even implicate market stability.

Blocking Consumers from Help

18. During my tenure as Chief Technologist and Senior Advisor to the Director at CFPB, I worked closely with the consumerfinance.gov and consumer education teams to develop strategies that ensured that the Bureau's content reached people when they most needed it, even if they had not heard of CFPB. Using desk research, the team identified the key areas where consumers commonly sought out information about topics such as avoiding scams and shopping for mortgages – most consumers start on search engines. To address this, we implemented an open standard schema that allowed search engines to index CFPB's content, ensuring that the most common consumer questions appeared prominently in search results, including "Position Zero" or "P0" rankings. Search results with "P0" ranking are often featured snippets that directly answer consumer queries on the results page, and were critically important in preventing and interrupting fraud and scams by making reliable, government-backed information the top result.

19. On February 7th, 2025, the CFPB homepage at consumerfinance.gov—the launching pad for most American consumers' interactions with the CFPB—was changed to a "404 - Site Not Found" error message.

20. I have been reliably informed that the decision to delete the CFPB homepage was an intentional decision by Acting Director Vought and that efforts by staff to repair the homepage were expressly rebuffed by senior management, citing Vought's authority.

21. This error, particularly when it affects the homepage of a website, can have severe repercussions. Specifically, it significantly harms the accessibility of important consumer information that the CFPB provides. A "404 error" on a homepage results in the following

detrimental effects:

- **Poor Experience:** When someone lands on a 404 page on the homepage, they are immediately presented with a frustrating experience. Consumers, particularly those seeking important financial information or assistance, will likely abandon the site.
- **Indexing Issues:** Search engine crawlers rely on accessible pages to index and rank content. A 404 error on the homepage can prevent crawlers from properly accessing the site, thereby hindering the search engines' ability to index the Bureau's important financial resources. This directly impacts the site's ability to appear in search results, making it more difficult for consumers to find reliable, government-backed financial information.

22. Since the implementation of the 404 error on the homepage of consumerfinance.gov on February 7th, 2025, the Bureau's web content—ranging from important in-the-moment guidance on financial abuse for victims of domestic violence, to help for military servicemembers to assert their rights under the Servicemembers' Civil Relief Act—has been removed from the most visible results despite no other changes to the site or schema. Those top results have been replaced in some cases by content farms or worse, scam sites. This is a direct consequence of the 404 error disrupting CFPB's search engine visibility, leaving vulnerable consumers to be targeted by fraudulent actors instead of receiving accurate, reliable information from the Bureau. This disruption is not just a technical oversight; it is a direct risk to consumer protection efforts, as the Bureau's content is now being supplanted by potentially harmful, deceptive websites.

23. These changes are in direct opposition to the statutory goal of providing consumers with timely and understandable information to make responsible decisions about financial transactions under 12 U.S.C. § 511(b). This unnecessary action—breaking the homepage of this federal consumer protection agency to a 404 error page—has had a profoundly negative impact on

the ability of the CFPB to meet consumers where they are in their moments of need, especially when they are seeking to protect themselves from fraud and make informed financial decisions. My years of experience and working directly with consumers looking for help inform my belief that people are being irreparably harmed when they are looking for help and instead find scams.

24. I am concerned that by breaking functionality of the website and in fact making it harder for consumers to access the critical financial information that they seek, recent actions have made it impossible for the Bureau to comply with its statutory obligation to maintain a consumer-facing website under 12 U.S.C. § 5493(b)(3).

“Your Recent or Impending Separation[s]”

25. In recent days, when employees have emailed the Bureau’s Human Relations (HR) staff with questions, they have received an unusual mass auto-response email indicating that the office will eventually address “your recent or impending separation.” A true and correct PDF copy of such an auto-response email that I received in response to an inquiry is attached as **Exhibit B**.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed in Washington, DC on February 27, 2025

/s/ Erie Meyer
Erie Meyer

EXHIBIT A

Mass Cancellation of CFPB Cyber Security Contracts

Prepared 2/27/25

The list below is taken from [doge.gov/savings](https://www.doge.gov/savings) and reflects 32 cyber security contracts they report having mass cancelled. The confirmed dates are as listed in the Federal Procurement Data System, and the unknown dates appear to have been cancelled sometime after 2/13. The doge site is experiencing lags and has evidence of backdating. The contracts below are listed on the doge site as having been "uploaded" on 2/14, but they were not listed before 2/18..

The work these contracts included protecting personally identifiable information, system integrity, and maintaining audit logs, among other critical security services.

| | Contract | Cybersecurity Impact | Date of cancellation |
|---|--|--|----------------------|
| 1 | BEYONDTRUST LICENSES | Identity and access management software | 2/13/25 |
| 2 | YUBI ENTERPRISE COMPLIANCE TIER PLUS PLAN | Physical 2FA keys issued to employees + software | 2/13/25 |
| 3 | CYBERSECURITY SUPPORT SERVICES - INFORMATION SECURITY STANDARDS (ISS) | Cybersecurity contractors | 2/13/25 |
| 4 | CYBERSECURITY SUPPORT SERVICES BPA ORDER - SAFEGUARDS AND RISK MANAGEMENT (SRM) | Cybersecurity contractors | 2/13/25 |
| 5 | CYBERSECURITY SUPPORT SERVICES BPA ORDER - SECURITY ARCHITECTURE AND ENGINEERING (SAE) | Cybersecurity contractors for SAE - team that performs cybersecurity review of new systems & sets required mitigations for ATO | 2/13/25 |
| 6 | CLOUD TRAINING | Technical training on cloud environments including cyber / cloud security and certification courses | Unknown |

| | | | |
|----|--|--|---------|
| 7 | <u>CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) IN-PERSON TRAINING</u> | CISA training | Unknown |
| 8 | <u>EZPROTECT SERVICES</u> | Virus scanning and cybersecurity for SaaS services | Unknown |
| 9 | <u>CENTRALIZED PLATFORM CONTROL STANDARDS SUPPORT SERVICES</u> | Cybersecurity contractors | Unknown |
| 10 | <u>ANOMALI LICENSES FOR CFPB</u> | Security Event & Information Management (SIEM) platform | Unknown |
| 11 | <u>SOLARWINDS MAINTENANCE AND SUPPORT</u> | IT network, systems, and applications management | Unknown |
| 12 | <u>NUTANIX HARDWARE DESKTOP ENGINEERING LAB SYSTEM UPGRADE</u> | Management platform for IT hardware deployment and configuration | Unknown |
| 13 | <u>CISCO SMARTNET MAINTENANCE</u> | Security alerts, updates, and tech support for core network equipment | Unknown |
| 14 | <u>ZIXGATEWAY ENTERPRISE LICENSE RENEWAL</u> | Email server security & encryption | Unknown |
| 15 | <u>ACCELLION KITEWORKS ENTERPRISE</u> | Secure file share / transfer services | Unknown |
| 16 | <u>VERACODE SERVICE BUNDLE SUBSCRIPTION</u> | Application security - code vulnerability scanning and penetration testing | Unknown |
| 17 | <u>SECUREAUTH IDP LICENSE RENEWAL</u> | Identity and access management - single sign on | Unknown |
| 18 | <u>AXONIUS SECURITY ASSET MANAGEMENT PLATFORM</u> | Centralized tracking / reporting for cyber vulnerability across IT hardware and software | Unknown |
| 19 | <u>CISCO ANYCONNECT LICENSE AND SUPPORT RENEWAL</u> | VPN on laptops issued to employees | Unknown |
| 20 | <u>ANNUAL SUBSCRIPTION TO THE BITSIGHT LARGE TPRM PACKAGE</u> | Third Party Risk Management (TPRM) - vendor security assessment, monitoring, and reporting | Unknown |

| | | | |
|----|---|--|---------|
| 21 | <u>CYBERARK ENTERPRISE LICENSES AND MAINTENANCE</u> | Identity security - manage, rotate, and monitor application credentials / secret keys | Unknown |
| 22 | <u>RADIANT LOGIC LICENSES</u> | Identity data management and audit | Unknown |
| 23 | <u>PUPPET LABS RENEWAL</u> | Centralized management, tracking, and enforcement of security configuration across IT infrastructure | Unknown |
| 24 | <u>CISCO AND NUTANIX HARDWARE AND SOFTWARE</u> | Network, hardware, and datacenter management | Unknown |
| 25 | <u>SAFECONSOLE ENTERPRISE LICENSES</u> | Provision, manage, and audit secure encrypted USB drives | Unknown |
| 26 | <u>VIRUSTOTAL BASIC SUBSCRIPTION</u> | Website and file virus scanning | Unknown |
| 27 | <u>QMULOS AUDIT/COMPLIANCE APPS</u> | Cybersecurity audit / event log analysis | Unknown |
| 28 | <u>TENABLE LICENSES AND SCANNER</u> | Network and application vulnerability scanning | Unknown |
| 29 | <u>IT DEVICE DESTRUCTION</u> | Secure equipment disposal | Unknown |
| 30 | <u>SAFECONSOLE LICENSES</u> | Provision, manage, and audit secure encrypted USB drives | Unknown |
| 31 | <u>KNOWB4 SUBSCRIPTION</u> | Online provider of bureau-wide mandatory cybersecurity training | Unknown |
| 32 | <u>ORDER 1 - CYBER PROGRAM MANAGEMENT</u> | Cybersecurity contractors | Unknown |

EXHIBIT B

Automatic reply: Question about my HR docs



Inbox x



CFPBHROps <CFPBHROps@fiscal.treasury.gov> Wed, Feb 19, 12:30 PM (8 days ago)
to me ▾



We are working diligently with the agency during this transition to provide necessary documents related to your recent or impending separation.

Please provide a personal email address and updated mailing address to ensure timely and effective communications.

All separated employees will be receiving a copy of their SF-50, Notice of Personnel Action, as well as a separation packet with information regarding unemployment, benefits and lump sum annual leave payment, if applicable.

Employees will have a 31-day extension of their health insurance from the date of separation provided by your health insurance carrier at no cost to you. Dental and Vision benefits will terminate upon the date of separation.

Thank you for your patience.

↩ Reply

➡ Forward



EXHIBIT A

Mass Cancellation of CFPB Cyber Security Contracts

Prepared 2/27/25

The list below is taken from [doge.gov/savings](https://www.doge.gov/savings) and reflects 32 cyber security contracts they report having mass cancelled. The confirmed dates are as listed in the Federal Procurement Data System, and the unknown dates appear to have been cancelled sometime after 2/13. The doge site is experiencing lags and has evidence of backdating. The contracts below are listed on the doge site as having been “uploaded” on 2/14, but they were not listed before 2/18..

The work these contracts included protecting personally identifiable information, system integrity, and maintaining audit logs, among other critical security services.

| | Contract | Cybersecurity Impact | Date of cancellation |
|---|--|--|----------------------|
| 1 | BEYONDTRUST LICENSES | Identity and access management software | 2/13/25 |
| 2 | YUBI ENTERPRISE COMPLIANCE TIER PLUS PLAN | Physical 2FA keys issued to employees + software | 2/13/25 |
| 3 | CYBERSECURITY SUPPORT SERVICES - INFORMATION SECURITY STANDARDS (ISS) | Cybersecurity contractors | 2/13/25 |
| 4 | CYBERSECURITY SUPPORT SERVICES BPA ORDER - SAFEGUARDS AND RISK MANAGEMENT (SRM) | Cybersecurity contractors | 2/13/25 |
| 5 | CYBERSECURITY SUPPORT SERVICES BPA ORDER - SECURITY ARCHITECTURE AND ENGINEERING (SAE) | Cybersecurity contractors for SAE - team that performs cybersecurity review of new systems & sets required mitigations for ATO | 2/13/25 |
| 6 | CLOUD TRAINING | Technical training on cloud environments including cyber / cloud security and certification courses | Unknown |

| | | | |
|----|--|--|---------|
| 7 | <u>CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) IN-PERSON TRAINING</u> | CISA training | Unknown |
| 8 | <u>EZPROTECT SERVICES</u> | Virus scanning and cybersecurity for SaaS services | Unknown |
| 9 | <u>CENTRALIZED PLATFORM CONTROL STANDARDS SUPPORT SERVICES</u> | Cybersecurity contractors | Unknown |
| 10 | <u>ANOMALI LICENSES FOR CFPB</u> | Security Event & Information Management (SIEM) platform | Unknown |
| 11 | <u>SOLARWINDS MAINTENANCE AND SUPPORT</u> | IT network, systems, and applications management | Unknown |
| 12 | <u>NUTANIX HARDWARE DESKTOP ENGINEERING LAB SYSTEM UPGRADE</u> | Management platform for IT hardware deployment and configuration | Unknown |
| 13 | <u>CISCO SMARTNET MAINTENANCE</u> | Security alerts, updates, and tech support for core network equipment | Unknown |
| 14 | <u>ZIXGATEWAY ENTERPRISE LICENSE RENEWAL</u> | Email server security & encryption | Unknown |
| 15 | <u>ACCELLION KITEWORKS ENTERPRISE</u> | Secure file share / transfer services | Unknown |
| 16 | <u>VERACODE SERVICE BUNDLE SUBSCRIPTION</u> | Application security - code vulnerability scanning and penetration testing | Unknown |
| 17 | <u>SECUREAUTH IDP LICENSE RENEWAL</u> | Identity and access management - single sign on | Unknown |
| 18 | <u>AXONIUS SECURITY ASSET MANAGEMENT PLATFORM</u> | Centralized tracking / reporting for cyber vulnerability across IT hardware and software | Unknown |
| 19 | <u>CISCO ANYCONNECT LICENSE AND SUPPORT RENEWAL</u> | VPN on laptops issued to employees | Unknown |
| 20 | <u>ANNUAL SUBSCRIPTION TO THE BITSIGHT LARGE TPRM PACKAGE</u> | Third Party Risk Management (TPRM) - vendor security assessment, monitoring, and reporting | Unknown |

| | | | |
|----|---|--|---------|
| 21 | <u>CYBERARK ENTERPRISE LICENSES AND MAINTENANCE</u> | Identity security - manage, rotate, and monitor application credentials / secret keys | Unknown |
| 22 | <u>RADIANT LOGIC LICENSES</u> | Identity data management and audit | Unknown |
| 23 | <u>PUPPET LABS RENEWAL</u> | Centralized management, tracking, and enforcement of security configuration across IT infrastructure | Unknown |
| 24 | <u>CISCO AND NUTANIX HARDWARE AND SOFTWARE</u> | Network, hardware, and datacenter management | Unknown |
| 25 | <u>SAFECONSOLE ENTERPRISE LICENSES</u> | Provision, manage, and audit secure encrypted USB drives | Unknown |
| 26 | <u>VIRUSTOTAL BASIC SUBSCRIPTION</u> | Website and file virus scanning | Unknown |
| 27 | <u>QMULOS AUDIT/COMPLIANCE APPS</u> | Cybersecurity audit / event log analysis | Unknown |
| 28 | <u>TENABLE LICENSES AND SCANNER</u> | Network and application vulnerability scanning | Unknown |
| 29 | <u>IT DEVICE DESTRUCTION</u> | Secure equipment disposal | Unknown |
| 30 | <u>SAFECONSOLE LICENSES</u> | Provision, manage, and audit secure encrypted USB drives | Unknown |
| 31 | <u>KNOWB4 SUBSCRIPTION</u> | Online provider of bureau-wide mandatory cybersecurity training | Unknown |
| 32 | <u>ORDER 1 - CYBER PROGRAM MANAGEMENT</u> | Cybersecurity contractors | Unknown |

EXHIBIT B

Automatic reply: Question about my HR docs



Inbox x



CFPBHROps <CFPBHROps@fiscal.treasury.gov> Wed, Feb 19, 12:30 PM (8 days ago)



to me ▾

We are working diligently with the agency during this transition to provide necessary documents related to your recent or impending separation.

Please provide a personal email address and updated mailing address to ensure timely and effective communications.

All separated employees will be receiving a copy of their SF-50, Notice of Personnel Action, as well as a separation packet with information regarding unemployment, benefits and lump sum annual leave payment, if applicable.

Employees will have a 31-day extension of their health insurance from the date of separation provided by your health insurance carrier at no cost to you. Dental and Vision benefits will terminate upon the date of separation.

Thank you for your patience.

↩ Reply

➡ Forward

