

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA)	CRIMINAL NO.
)	
)	VIOLATIONS:
v.)	
)	Wire Fraud
)	18 U.S.C. §§ 1343 and 2(a)
DANIELLE HILLMER,)	
)	Major Fraud
)	18 U.S.C. §§ 1031 and 2(a)
Defendant.)	
)	Obstruction of a Federal Audit
)	18 U.S.C. §§ 1516 and 2(a)

INDICTMENT

THE GRAND JURY CHARGES:

Introductory Allegations

At times relevant to this Indictment, unless otherwise stated:

1. Company A was a government contractor headquartered in Virginia that provided, among other things, cloud computing services to federal government agencies. From in or around 2017, through at least in or around 2022, Company A sold a cloud service that was marketed as a secure, cloud-based platform (the “Platform”). Company A’s Platform customers included the Department of the Army (the “Army”), Department of Veterans Affairs, Department of State, and other government agencies.

2. Defendant **DANIELLE HILLMER** was a resident of Chantilly, Virginia. She was employed as a senior manager for Company A. From at least in and around November 2018, through at least in and around November 2021, **HILLMER** was the person responsible for oversight of assessments, authorizations, and continuous monitoring of the Platform.

3. Employee 1 was an associate manager for Company A. From in or around May 2020, through in or around June 2021, Employee 1 was the security and compliance lead for the Platform and the person responsible for maintaining the appropriate operational security posture for the Platform.

4. Employee 2 was a senior manager for a subsidiary of Company A. From in or around September 2019, until his departure from the company in or around May 2020, Employee 2 served as a cyber security consultant for the Platform and reported to **HILLMER**. Employee 2 returned to Company A and replaced Employee 1 as the security and compliance lead for the Platform in or around October 2021.

5. From approximately March 2020, and continuing through at least November 2021, **HILLMER** engaged in a scheme to defraud the United States and its departments and agencies by making false and misleading representations about the Platform's security and risk posture to help Company A obtain and maintain lucrative federal contracts. The scheme was executed in two ways: first, by obstructing federal auditors to fraudulently obtain and maintain government authorization to operate the Platform, and second, by making false representations to maintain government contracts and obtain payments from the government to benefit Company A.

Assessment and Authorization Requirements for Cloud Service Offerings

FedRAMP Requirements

6. The Federal Risk and Authorization Management Program ("FedRAMP") was a government-wide program that provided a standardized approach for assessing, authorizing, and continuously monitoring the security of cloud products and services as a prerequisite for use by the federal government.

7. The General Services Administration (“GSA”) was a federal agency headquartered in the District of Columbia that administered FedRAMP.

8. The Joint Authorization Board (“JAB”) was a governing body for FedRAMP comprised of representatives from the GSA, Department of Defense (“DoD”), and Department of Homeland Security (“DHS”).

9. FedRAMP established uniform security requirements for cloud services based on the sensitivity and criticality of information processed, stored, or generated by the system. Under FedRAMP, there were three risk impact levels: Low, Moderate, and High. To hold federal information, cloud service offerings were required to obtain an authorization to operate (“ATO”) at the relevant risk impact level and demonstrate continuous compliance with FedRAMP security requirements, called “security controls,” through mandatory monitoring, reporting, and assessments.

10. FedRAMP continuous monitoring requirements included tracking vulnerabilities in a Plan of Action & Milestones (“POA&M”) submitted to FedRAMP at least monthly. Continuous monitoring was critical, because it provided authorizing officials and federal agencies using cloud services a method to determine if the system security was operating as intended and to detect changes to the security posture of the system for the purpose of making risk-based decisions.

11. FedRAMP required that a third-party assessment organization (“3PAO”) test cloud service offerings’ implementation of security controls at three critical stages in the FedRAMP authorization process: (a) prior to obtaining an initial authorization, (b) annually to maintain an authorization, and (c) prior to a “significant change” to the system. A “significant change” was a change likely to affect the security state of the information system, such as an uplift from FedRAMP Moderate to High.

12. FedRAMP assessments were federal audits. During an assessment, the 3PAO would gather physical artifacts and participate in live demonstrations to test the cloud service offerings' implementation of security controls. Evidence and results from 3PAO assessments were incorporated into assessment and authorization packages submitted to FedRAMP and authorizing officials for review and approval, which were made available to current and prospective government customers.

13. FedRAMP assessment and authorization information and materials were generally transmitted to government officials via an online portal, the Office of Management and Budget's MAX Information System ("MAX") and stored within the District of Columbia.

Department of Defense Requirements

14. In addition to FedRAMP, DoD implemented its own risk management framework with a separate authorization process and approval requirements for cloud products or services sold to DoD.

15. Cloud service offerings could obtain a DoD provisional authorization ("PA") by leveraging an existing FedRAMP authorization and demonstrating compliance with additional DoD-specific requirements based on the impact level of the data to be hosted. The DoD authorization process began at the request of a sponsor, the DoD component requiring the cloud service, and involved a review of the security authorization package, assessments, and continuous monitoring submissions.

16. DoD had six impact levels denoting the sensitivity of the data to be hosted, from DoD Impact Level ("IL") 1 to 6. DoD IL2 information could be hosted in a system with authorization at the FedRAMP Moderate baseline. DoD IL4 and above required a combination of

FedRAMP Moderate, FedRAMP High, and DoD-specific security controls. DoD IL5 represented the highest security classification within the DoD framework for unclassified information systems.

Army NIFMS Contract

17. In or around November 2018, the Army Installation Management Command awarded a contract to Company A for the delivery of the Nonappropriated Fund Integrated Financial Management System (“NIFMS”), a cloud-based payroll, pension, and benefits system. The base award was a five-year, firm fixed price, Indefinite Delivery/Indefinite Quantity (“IDIQ”) contract. The Army maintained its contract with Company A through task orders that were awarded for specific work to be performed at different phases including, but not limited to, the following:

Task Order No.	Description	Approx. Value
NAFBA1-20-F-0149	Increment 2	\$8,342,568
NAFBA1-21-F-0017	Increment 3	\$20,265,599
NAFBA1-21-F-0141	Software	\$1,092,775

The IDIQ contract and all task orders awarded to Company A for NIFMS are collectively referred to as the “NIFMS Contract.”

18. The NIFMS Contract required Company A to obtain a DoD PA at DoD IL4 and maintain security controls to meet DoD IL4 and DoD-specific Privacy and Financial Management Overlays. Those security controls were required due to the highly sensitive nature of the data to be stored in NIFMS, including personally identifiable information and financial data for thousands of Army employees, pensioners, and survivors. Company A’s ability to obtain and maintain a DoD PA at DoD IL4 was essential to performance of the NIFMS Contract.

Scheme to Defraud the United States

19. From approximately March 2020, and continuing through at least November 2021, **HILLMER**, and others known and unknown to the Grand Jury, engaged in a scheme to defraud the United States by making false and misleading representations about the Platform's security and risk posture to help Company A obtain and maintain lucrative federal government contracts.

Purpose of the Scheme

20. The purpose of the defendant's scheme was to fraudulently obtain contracts and payments from the government to benefit Company A, and unlawfully enrich herself through continued compensation in salary and bonuses from Company A, by making, and aiding and abetting the making of, materially false and misleading statements to, among other things: (a) fraudulently obtain and maintain a FedRAMP High P-ATO; (b) fraudulently induce the Army to award task orders to Company A and sponsor the Platform for a DoD IL4 PA; and (c) conceal the true state of the Platform from assessors, authorizing officials, and government customers.

Manner and Means of the Scheme

21. The manner and means by which **HILLMER** sought to accomplish the purpose of the scheme included, but were not limited to, the following:

22. **HILLMER** sought JAB authorization to uplift the Platform from FedRAMP Moderate to High, which Company A intended to leverage to obtain a DoD PA at IL5. **HILLMER** understood that Company A had a contractual requirement to provide a DoD IL4 environment to the Army and had potential DoD customers with IL5 requirements.

23. Despite receiving repeated warnings from employees and outside consultants that the Platform was not ready for the uplift, **HILLMER** made false and misleading representations about the system architecture and implementation of security controls to assessors and authorizing

officials to fraudulently obtain approval to uplift the Platform to FedRAMP High. Among other things, **HILLMER** knew the Platform had not implemented required security controls related to access control, incident response, and continuous monitoring, including auditing, logging, monitoring, and alerting. **HILLMER** also knew customer environments were not managed, monitored, governed, and secured as represented in the Platform's System Security Plan.

24. **HILLMER** endeavored to influence, obstruct, and impede auditors in the performance of their official duties by making, and aiding and abetting the making of, representations and submissions that she knew contained materially false and misleading representations about the implementation of security controls and instructing others to conceal the true state of the system from assessors.

25. **HILLMER** submitted or caused the submission of assessment and authorization materials that she knew contained materially false and misleading information about the Platform's architecture, implementation of security controls, and overall security posture, to assessors, authorizing officials, and government customers via MAX and a web-based application utilized by the 3PAO.

26. **HILLMER** fraudulently induced the Army to sponsor the Platform for a DoD PA based on materially false and misleading representations about the Platform's architecture, technical capabilities, and compliance with DoD IL4 requirements, and submitted or caused the submission of false and misleading assessment and authorization materials to the Army via eMASS, a web-based application utilized by DoD.

27. These deceptive acts enabled Company A to fraudulently obtain and retain government authorization to operate the Platform and government contracts that required a level of security that the Platform did not actually provide.

Executing the Scheme to Defraud

28. On or about March 10, 2020, **HILLMER** signed and caused a Significant Change Request to be submitted to FedRAMP and the JAB, via MAX, seeking approval to implement new technology and uplift the Platform from FedRAMP Moderate to High. The request stated that the change was driven by awarded contracts with the Army, which were contingent on achieving FedRAMP High. **HILLMER** represented to the JAB that FedRAMP High controls would be implemented by April 2020 and operational by August 31, 2020.

29. On or about at least April 29, 2020, and continuing through May 21, 2020, Employee 2 repeatedly warned **HILLMER** and others at Company A that the Platform was not compliant with security requirements and identified risks associated with an uplift to FedRAMP High and DoD IL5, including deficient access controls that would be “serious auditor red flags that may impact our ATO.”

30. On or about June 2, 2020, an outside firm engaged by **HILLMER** to prepare system security plans and related documentation in preparation for the uplift warned **HILLMER** that the Platform was not ready for the uplift because more than 100 security controls and DoD general readiness requirements were not implemented, and for various controls, a solution had not yet been determined.

31. On or about July 10, 2020, despite knowing that the system was still being designed and the Platform lacked the resources and technical capabilities to implement the security controls required for FedRAMP High, **HILLMER** approved the submission of a FedRAMP High

Readiness Assessment Report (“RAR”), via MAX, to deceive FedRAMP and the JAB to approve the High uplift.

32. Between approximately June and December 2020, during and in connection with assessments of the Platform’s implementation of security controls at FedRAMP Moderate, High, and DoD IL5 (the “2020 Assessment”), **HILLMER** concealed known issues from assessors and authorizing officials and failed to correct false and misleading representations made in statements and submissions to assessors and authorizing officials.

33. On or about September 28, 2020, **HILLMER** caused a Significant Change Request to be submitted to FedRAMP and the JAB, via MAX, which sought approval for the High uplift and falsely represented that all FedRAMP High controls were implemented. **HILLMER** represented that Company A sought the High uplift to meet its contractual obligations to the Army and other government customers and that the elevated compliance level must be operational by January 1, 2021.

34. In and around November and December 2020, **HILLMER** caused FedRAMP assessment and authorization materials to be submitted to FedRAMP and the JAB, via MAX, knowing they contained materially false and misleading representations about the Platform’s architecture, implementation of security controls, and risk posture. Among other things, **HILLMER** knew that customer environments were not managed, monitored, governed, and secured as represented in the Platform’s System Security Plan, Security Assessment Reports, and continuous monitoring.

35. On or about January 20, 2021, and on or about January 28, 2021, **HILLMER** signed a service level agreement (“SLA”), whereon **HILLMER** knowingly made materially false

representations, including that the Platform complied with the Army's DoD IL4 requirements and "currently maintains enhanced controls to meet the requirements of an IL5 environment."

36. On or about May 18, 2021, **HILLMER** submitted materially false and misleading information to the Army via e-mail, including the Platform's DoD IL5 Security Assessment Plan and DoD FedRAMP+ Readiness Assessment Report.

37. On or about May 26, 2021, **HILLMER** submitted and caused the submission of materially false and misleading information to the Army, via eMASS, including the Platform's FedRAMP System Security Plan Version 5.0, dated January 29, 2021, DoD IL5 Addendum Version 1.0, dated June 12, 2020, DoD DISA SRG IL5 Security Assessment Report, Version 1.0, dated November 11, 2020, and POA&M for May 2021.

38. On or about June 23, 2021, in an email to members of her team, **HILLMER** acknowledged that administrators were accessing the Platform without the necessary multi-factor authentication, which was required for FedRAMP High and would be a problem if known to assessors. The same day, **HILLMER** requested a meeting with management at Company A about the 2021 Assessment, writing: "we need a 'Hale Mary [sic]" to pass the assessment.

39. Between approximately July 2021 and September 2021, during and in connection with an assessment of the Platform's implementation of security controls at FedRAMP High and DoD IL4 (the "2021 Assessment"), **HILLMER** concealed known issues from assessors and authorizing officials and failed to correct false and misleading representations made in statements and submissions to assessors and authorizing officials.

40. On or about July 12, 2021, in a private chat with **HILLMER** following a virtual demonstration for assessors, Employee 1 wrote: "we've dodged the [multi-factor authentication]

implementation bullet for now, but it could come up again ... We aren't out of the woods yet."

HILLMER replied with a fingers crossed emoji.

41. On or about July 27, 2021, **HILLMER** sent an email to FedRAMP requesting the status of the Platform's High P-ATO, because "[w]e have an existing customer who's [sic] Agency ATO is being held up because the [FedRAMP] Marketplace still lists us at the Moderate baseline." The same day, FedRAMP emailed **HILLMER** a signed letter from the JAB, granting the Platform a FedRAMP High P-ATO upon belief "[the Platform's] Security Authorization Package accurately documents and clearly defines the risk considerations" for federal agency customers. Upon receipt, **HILLMER** forwarded the authorization letter to the Army.

42. On or about August 19, 2021, on or about September 7, 2021, and on or about September 21, 2021, **HILLMER** made false and misleading representations to the Army and DoD officials about the Platform's architecture and implementation of security controls, in meetings as well as in written submissions as part of the process to obtain a DoD PA. On or about each of those dates, **HILLMER** e-mailed presentations to assessors, the Army, and DoD officials, which **HILLMER** knew falsely represented that the Platform maintained architectural components and technical capabilities that were neither implemented nor operational, then or at the time they were assessed in 2020.

43. From approximately 2020 and 2022, at least six United States departments and agencies, including the Army, used or planned to use the Platform's JAB P-ATO to obtain agency authorizations for cloud products and services provided by Company A, pursuant to contracts and subcontracts with the United States valued at more than \$250 million.

COUNTS ONE AND TWO
Wire Fraud
(18 U.S.C. §§ 1343 and 2(a))

44. Paragraphs 1 through 43 are hereby re-alleged and incorporated by reference as though fully set forth in this Count of the Indictment.

45. From approximately March 2020 and continuing through at least November 2021, in the District of Columbia, and elsewhere, the defendant,

DANIELLE HILLMER,

knowingly, and with the intent to defraud, devised and intended to devise a scheme to defraud the United States, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, knowing such pretenses, representations, and promises were false and fraudulent when made, transmitted and caused to be transmitted, by means of wire communications in interstate commerce, writings, signals, pictures, and sounds, for the purpose of executing the scheme.

Use of Interstate Wires

46. On or about the following dates, in the District of Columbia, and elsewhere, **HILLMER**, for the purpose of executing the scheme described above, and attempting to do so, knowingly transmitted and caused to be transmitted by means of wire communication in interstate commerce, a writing, sign, picture, and sound, each transmission constituting a separate count:

Count	Approx. Date	Description of Interstate Wire(s)
1	12/9/2020	Submission of FedRAMP assessment and authorization materials via MAX
2	5/4/2021	Submission of FedRAMP assessment and authorization materials via MAX

Each in violation of Title 18, United States Code, Sections 1343 and 2(a).

COUNT THREE
Major Fraud
(18 U.S.C. §§ 1031 and 2(a))

47. Paragraphs 1 through 43 are hereby re-alleged and incorporated by reference as though fully set forth in this Count of the Indictment.

48. From at least in or around March 2020, and continuing through at least in or around November 2021, within the District of Columbia, and elsewhere, the defendant,

DANIELLE HILLMER,

knowingly executed, and attempted to execute, a scheme and artifice with the intent to defraud the United States and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in procurements of property and services as a prime contractor on a contract with the United States with a value in excess of \$1 million; namely, the NIFMS Contract.

49. On or about July 27, 2021, in the District of Columbia, and elsewhere, **HILLMER** knowingly executed and attempted to execute this scheme to defraud by requesting, obtaining, and receiving a FedRAMP High P-ATO for Company A and the Platform, which was stored on MAX and reflected on the FedRAMP Marketplace.

In violation of Title 18, United States Code, Sections 1031 and 2(a).

COUNT FOUR
Obstruction of a Federal Audit
(18 U.S.C. §§ 1516 and 2(a))

50. Paragraphs 1 through 43 are hereby re-alleged and incorporated by reference as though fully set forth in this Count of the Indictment.

51. From in or around June 2020, and continuing through at least April 2021, in the District of Columbia, and elsewhere, the defendant,

DANIELLE HILLMER,

with the intent to deceive and defraud the United States, endeavored to influence, obstruct, and impede federal auditors, who defendant knew to be performing official duties relating to Company A, an entity receiving in excess of \$100,000, pursuant to contracts and subcontracts with the United States during any 12-month period in calendar years 2020 and 2021. Specifically, **HILLMER** made and aided and abetted the making of false and misleading representations and submissions to assessors and authorizing officials during and in connection with the 2020 Assessment of the Platform at FedRAMP Moderate, High, and DoD IL5 and employed deceptive tactics to conceal security controls and technical capabilities that were not implemented or operating as required.

In violation of Title 18, United States Code, Sections 1516 and 2(a).

COUNT FIVE
Obstruction of a Federal Audit
(18 U.S.C. §§ 1516 and 2(a))

52. Paragraphs 1 through 43 are hereby re-alleged and incorporated by reference as though fully set forth in this Count of the Indictment.

53. From in or around July 2021, and continuing through at least in or around September 2021, in the District of Columbia, and elsewhere, the defendant,

DANIELLE HILLMER,

with the intent to deceive and defraud the United States, endeavored to influence, obstruct, and impede federal auditors, who defendant knew to be performing official duties relating to Company A, an entity receiving in excess of \$100,000, pursuant to contracts and subcontracts with the United States during calendar year 2021. Specifically, **HILLMER** made and aided and abetted the making of false and misleading representations and submissions to assessors and authorizing officials during and in connection with the 2021 Assessment of the Platform at FedRAMP High

and DoD IL4 and employed deceptive tactics to conceal security controls and technical capabilities that were not implemented or operating as required.

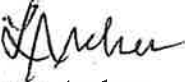
In violation of Title 18, United States Code, Sections 1516 and 2(a).

THIS IS A TRUE BILL.

Dated: December 9, 2025

FOREPERSON

LORINDA I. LARYEA
Acting Chief, Fraud Section
Criminal Division
United States Department of Justice

By: 

Lauren Archer
Paul Hayden
Trial Attorneys
Criminal Division, Fraud Section
United States Department of Justice