UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11323 / October 22, 2024

SECURITIES EXCHANGE ACT OF 1934
Release No. 101401 / October 22, 2024

ADMINISTRATIVE PROCEEDING
File No. 3-22272

In the Matter of **Unisys Corporation,** **Respondent.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 ("Securities Act") and Section 21C of the Securities Exchange Act of 1934 ("Exchange Act") against Unisys Corporation ("Unisys" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-And-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds[1] that:

Summary

1. This matter concerns materially misleading statements that Unisys, a global provider of technical and enterprise information technology ("IT") services and solutions to large commercial enterprises and public sector entities, including global non-profit organizations, foreign, state, and local governments, and, for a period, the U.S. government, negligently made regarding cybersecurity risks and events, as well as Unisys's violations of disclosure controls and procedures requirements.

2. In December 2020, Unisys identified one computer in its network that had a version of SolarWinds Orion software, which a likely nation-state threat actor[2] infected with malicious code that could have allowed for unauthorized activity on affected computers and their networks ("SolarWinds Compromise"). Unisys also received notifications about and discovered compromises of its environment likely by the same threat actor. The compromises of Unisys's systems took place over a combined span of at least sixteen months starting in January 2020 and were persistent and impacted several parts of its corporate network and non-customer facing cloud environment. Specifically, the activity involved the compromise of at least seven network credentials[3] and 34 cloud-based accounts, including those with administrative privileges, repeated connections into Unisys's network with at least 33 gigabytes ("GB") of data transferred, and access to cloud-based shared files and mailboxes, including those of senior IT personnel. Unisys was aware that its investigations of the compromise involved significant gaps in its ability to identify the full scope of the unauthorized activity due to the lack of availability of the forensic evidence.

3. Unisys filed with the Commission annual reports on Form 10-K for fiscal years ended December 31, 2020 and 2021 that included cybersecurity risk disclosures that were materially misleading and not sufficiently tailored to its particular risks and incidents. In these disclosures, Unisys inaccurately described the existence of successful intrusions and the risk of unauthorized access to data and information in hypothetical terms, despite knowing that the above-described

[1] The findings herein are made pursuant to Respondent's Offer and are not binding on any other person or entity in this or any other proceeding.

[2] The term "threat actor" refers to an individual, group, organization, or government that conducts or has the intent to conduct unauthorized activities against the networks and data of or used by others.

[3] The term "credential" refers to a username and password combination or key used to access resources on a network. Compromised credentials are used by threat actors to gain unauthorized access to these resources. Different credentials have varying levels of access to and privileges on the network. For instance, administrative credentials generally have broader access to the network or to specific systems or applications and allow the operator to take actions a standard user would not be able to take, such as adding new credentials or modifying the level of access for existing credentials, among other things, depending on the type of administrative credential. Generally, a threat actor that compromises more credentials and credentials with higher privileges will be more persistent and more difficult to eradicate from a network.

intrusions had actually happened and in fact involved unauthorized access and exfiltration of confidential and/or proprietary information.

4. Unisys's materially misleading statements resulted in part from the company's failure to design controls and procedures to ensure (1) that information about potentially material cybersecurity incidents was timely recorded, processed, summarized and reported, within the time period specified as appropriate in the Commission's rules and forms, and (2) that information was accumulated and communicated to the company's management to allow timely decisions regarding required disclosures. As a result, decision makers failed at the time to reasonably assess the materiality of these events and new risks arising therefrom.

5. Separately, in July 2022, a separate threat actor—a Russian-speaking ransomware group—successfully compromised Unisys's network and exfiltrated[4] certain cybersecurity and product and platform software code for products the company offers to its customers.

6. Before December 2022, Unisys's incident response policies did not reasonably require cybersecurity personnel to report information to Unisys's disclosure decision makers and contained no criteria for determining which incidents or information should be reported outside the information security organization. Consequently, Unisys's senior cybersecurity personnel repeatedly failed to report the above incidents to executive management and the legal department in a timely manner.

7. As discussed in greater detail below, Unisys has taken a number of remedial steps, including enhancing its incident response policies and procedures in December 2022 and augmenting its cybersecurity personnel and tools. Also, after investigating the 2022 extortion event and its cybersecurity controls, Unisys publicly disclosed a material weakness in its disclosure controls and procedures and internal control over financial reporting related to the design and maintenance of effective formal policies and procedures over information being communicated by the IT function and the legal and compliance function to those responsible for governance to allow timely decisions related to both financial reporting and other non-financial reporting.

8. Based on the foregoing conduct, and the conduct described herein below, Unisys violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, and 13a-15(a) thereunder.

Respondent

9. Unisys is a Delaware corporation with headquarters in Blue Bell**,** Pennsylvania. During all relevant times, its stock has traded on the New York Stock Exchange under the ticker symbol UIS, and its common stock was registered under Section 12(b) of the Exchange Act. Unisys is required to file with the Commission, among other things, annual reports on Form 10-K pursuant to Section 13 of the Exchange Act and Rule 13a-1 thereunder. Unisys's information technology network and resources regularly stored and transmitted its customers' data and information, in addition to Unisys's own data and code.

[4] The term "exfiltration" refers to the unauthorized transfer of data from an information system.

Facts

10. During the relevant time period, Unisys was a provider of technical and enterprise IT services and solutions to large commercial enterprises and public sector entities, including global non-profit organizations, foreign, state, and local governments, and, for a period, the U.S. government. It offered products and services for digital workplace solutions, cloud, applications and infrastructure solutions, and enterprise computing solutions.

SolarWinds Compromise-Related Activity

11. In December 2020, Unisys identified an infected version of the SolarWinds software on at least one computer in its network. In a subsequent investigation, it learned that the infected software was loaded on seven dates (but found no evidence that the malicious implant was exploited by the SolarWinds threat actor) and that two other computers made one internet connection each to a known malicious command-and-control server via an internet browser (rather than an installation of the SolarWinds software). At the time of Unisys's investigation, its logs and forensic evidence of possible compromise were insufficient to rule out unauthorized activity for some of the installations. The company retained a third-party service provider to review the available forensic evidence as well as additional forensic evidence the service provider maintained with respect to the Unisys network. The service provider did not identify evidence of exploitation or other additional activity involving the SolarWinds software or through the internet connections on the two computers, but recommended that the company conduct a forensic review of the three computers with evidence of potentially unauthorized activity. Unisys determined that the level and nature of known activity on these computers did not necessitate such additional investigation.

12. Throughout December 2020, Unisys learned that the threat actor behind the compromise of the SolarWinds Orion software was a hacking group likely associated with a nation-state. Public reports and commercial cybersecurity intelligence sources widely attributed the activity to the Russian Federation in late December 2020. On January 5, 2021, a joint public statement by the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the National Security Agency, and the Cybersecurity and Infrastructure Security Agency attributed the attack to an intelligence gathering operation "likely Russian in origin." The event impacted thousands of SolarWinds' customers.

13. On December 13, 2020, Unisys's then-senior cybersecurity personnel received credible information that likely the same threat actor had compromised Unisys's network and non-customer facing cloud environment using means other than SolarWinds software beginning in February 2020. The company's subsequent investigation uncovered evidence that the threat actor engaged in the following activities between January 2020 and February 2021: compromised at least three Unisys network user accounts and gained access to eight Unisys cloud-based user accounts, including accounts with global administrative privileges and the internal Unisys accounts of employees who serviced certain of the company's customers; repeatedly initiated and completed Virtual Private Network ("VPN") connections during which approximately 23GB of data was transferred to and approximately seven gigabytes was transferred from the company's network; and accessed the contents of at least five cloud-based mailboxes, including high-level IT personnel

and a Chief Information Officer for the company's then federal government business. Unisys took various remedial measures after investigating the activity.

14. In August 2021, Unisys received credible information that the same threat actor accessed the company's VPN and non-customer facing cloud environment again between April and August 2021. The company's investigation identified evidence of additional persistent unauthorized activity, compromise of least four network user accounts and 28 cloud-based accounts, access to 14 systems, repeated VPN sessions, and access to approximately 27,000 email messages and 130 cloud-based shared files. Unisys's policies did not include adequate escalation procedures in the event of a cybersecurity incident, and Unisys cybersecurity personnel did not report this activity to senior management. Unisys also failed to review the contents of the messages and shared files until 2022, by which point only half of these documents remained available. Between April and August 2021, the threat actor exploited information obtained in 2020 about the Unisys network and at least one persistence mechanism the threat actor established in 2020, an authorization certificate for facilitating authorization for cloud-based applications, which the company failed to identify during its review of the 2020 activity.

15. In April 2023, Unisys received yet another notification of unauthorized activity by likely the same threat actor. Unisys's investigation determined that the threat actor attempted but failed to access company resources at that time. However, after receipt of new information from law enforcement in May 2023, the company determined that the same threat actor accessed its non-customer facing cloud environment with administrative privileges for approximately a month, activity which Unisys was not aware of previously. During this activity, the threat actor again likely used another persistence mechanism it had established in 2020: a second authorization certificate introduced in 2020, which allowed the threat actor to grant administrative privileges to an application in 2023, and which Unisys failed to identify during its review of the 2020 and 2021 activity. Unisys's cybersecurity personnel reported this activity to senior management the same day they received the notification.

16. Unisys's investigations of these incidents consisted of reviewing forensic evidence on the infected computers and logs of network and cloud activity. However, at the time of the investigations, the company lacked visibility into the incidents due to a number of factors. For example, the company could not identify all of the relevant activity and mechanisms of persistence because it did not have access to logs and forensic evidence covering the full scope of the activity.

Unisys's Materially Misleading Cybersecurity Risk Disclosures

17. As a provider of technical and enterprise IT services and solutions to large commercial enterprises and public sector entities, including global non-profit organizations; foreign, state, and local governments; and, for a period, the U.S. government, Unisys's ability to protect information and data stored on and transmitted over its network was critically important to its reputation and ability to attract and retain customers and to investors. Moreover, Unisys's information and data were of great interest to state-sponsored cyber threat actors, such as the threat actor likely behind the SolarWinds Compromise.

18. Unisys's cybersecurity risk profile changed materially as a result of the SolarWinds Compromise-related activity for the following reasons: (1) a persistent and reportedly nation-state-

supported threat actor compromised the company's environment; (2) the threat actor persisted in the environment unmonitored for a combined span of at least sixteen months; and (3) the company's investigation of the activity suffered from gaps that prevented it from identifying the full scope of the compromise.

19. On February 26, 2021 and February 22, 2022, Unisys filed its annual reports for the years ending 2020 and 2021, respectively, on Form 10-K with the Commission. In both reports, Unisys negligently framed risks from cybersecurity events as hypothetical despite the company's awareness of the SolarWinds Compromise-related activity, thereby rendering these disclosures materially misleading. For example, these disclosures stated that cyberattacks "*could* … result in the loss … or the unauthorized disclosure or misuse of information of the company" and that *"[i]f our systems are accessed* without our authorization … *we could* … experience data loss and impediments to our ability to conduct our business, and damage the market's perception of our services and products." (Emphasis added). Moreover, Unisys's disclosures on Forms 10-K for years 2020 and 2021 were substantially unchanged from those on its Form 10-K for 2019, which were made before discovering the information described above about the SolarWinds Compromise-related activity.

20. Throughout the periods discussed above, including following the filing of the above-discussed Forms 10-K for the years ending 2020 and 2021, Unisys offered and sold securities to certain of its employees through grants of restricted stock units.

2022 Extortion Event

21. Between July 7 and 12, 2022, Unisys's internal cybersecurity systems issued at least 10 alerts about the presence and execution of powerful password-stealing malware, Mimikatz, on seven computers in its non-customer facing software development network. Unisys's cybersecurity personnel were not sufficiently familiar with the format of the alerts and erroneously believed that the malware was deployed on only one machine and only on July 7, 2022. The company's cybersecurity personnel also assigned a low priority to the activity because one of the alerts stated that the malware was quarantined. As a result, no cybersecurity personnel took steps to investigate the activity until July 13, almost a week after the initial alert.

22. Unisys's cybersecurity personnel determined on July 14, 2022 that the malware was not in fact quarantined, and it conducted additional investigation and identified an active intrusion by another threat actor, a Russian-speaking ransomware group. The next day, Unisys took the compromised lab network off the internet. However, during the eight days between the initial alerts and Unisys's disconnection of the network, the threat actor exfiltrated certain cybersecurity and product and platform software code for products the company offers to its customers. Unisys notified criminal law enforcement as part of its incident response.

23. By July 22, 2022, Unisys identified evidence of this code exfiltration and in fact found a copy of the code on a threat actor-controlled server on the internet. Unisys cybersecurity personnel initially believed that they were able to remove the code from the threat actor-controlled server. However, on July 25 and 30, 2022, the threat actor provided evidence to Unisys that it still had a copy of the code. In addition, on August 3, 2022, in an effort to pressure Unisys into paying a ransom, the threat actor briefly posted on its darkweb site a message alleging that it had

exfiltrated all of Unisys's code. The post was up for less than one hour and did not receive media coverage.

24. In the course of the incident, Unisys discovered that its endpoint detection and response system was not set up properly to automatically send alerts to its centralized Security Information and Event Management system, which Unisys's policies and procedures required to be monitored regularly by cybersecurity personnel. Unisys was unable to determine how long the misconfiguration persisted and how many alerts were not reviewed by cybersecurity personnel as a result.

25. On November 21, 2022, after investigating the 2022 extortion event and its cybersecurity controls, Unisys filed with the Commission a Form 8-K that disclosed a material weakness in its disclosure controls and procedures and internal control over financial reporting related to the design and maintenance of effective formal policies and procedures over information being communicated by the IT function and the legal and compliance function to those responsible for governance to allow timely decisions related to both financial reporting and other non-financial reporting. Unisys also implemented certain remediation measures.

Unisys's Failure to Maintain Disclosure Controls and Procedures

26. Unisys's cybersecurity personnel failed to report the 2020 and 2021 activity to disclosure decision-makers until a year after discovering it, and the 2022 extortion incident until the hackers' public statement. At the time of these events, Unisys did not maintain effective controls requiring escalation of potentially material incidents to senior management and disclosure decision-makers. At the same time, Unisys did not have controls and procedures designed to ensure that its disclosure decision-makers reviewed cybersecurity incident information in Unisys's possession in order to determine which information about the incident may be required to be disclosed in Commission filings. Accordingly, despite the importance of data integrity and confidentiality to Unisys, the company failed to maintain disclosure controls and procedures designed to ensure that information around material cybersecurity incidents was, among other things, reported to management responsible for disclosures and therefore timely reported to investors. Specifically, Unisys's deficient controls contributed to Unisys's materially misleading risk factor disclosures for the years ending 2020 and 2021.

27. Following its disclosure of a material weakness on November 21, 2022, Unisys took steps to remediate its control deficiencies, including enhancing cyber-related policies and procedures and augmenting its cybersecurity personnel and tools, both internally and externally.

Violations

28. As a result of the conduct described above, Unisys violated Section 17(a)(2) of the Securities Act, which proscribes, in the offer or sale of a security, obtaining "money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading."

29. As a result of the conduct described above, Unisys violated Section 17(a)(3) of the Securities Act, which makes it unlawful for any person in the offer or sale of a security to engage "in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser."[5]

30. As a result of the conduct described above, Unisys violated Section 13(a) of the Exchange Act and Rule 13a-1 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission annual reports in conformity with the Commission's rules and regulations. Unisys also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in annual reports filed with the Commission any material information necessary to make the required statements in the filing not misleading.

31. As a result of the conduct described above, Unisys violated Exchange Act Rule 13a-15(a), which requires issuers with a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.

Unisys's Cooperation

32. In determining to accept the Offer, the Commission considered remedial acts undertaken by Unisys and Unisys's cooperation afforded the Commission staff. This cooperation included providing the staff with several lengthy and detailed presentations, as well as summaries of specific factual issues and additional information, which furthered the efficiency of the staff's investigation. In addition, Unisys took certain steps to remediate its control deficiencies, including enhancing disclosure policies and procedures and augmenting its cybersecurity personnel and tools, both internally and externally, to strengthen its cybersecurity risk management and protections.

Undertakings

Unisys has undertaken to complete the following actions:

Cooperation

33. Unisys undertakes to cooperate fully with the Commission in any and all investigations, litigations or other proceedings relating to or arising from the matters described in the Order.

[5] Negligence is sufficient to establish violations of Sections 17(a)(2) and 17(a)(3). *Aaron v. SEC*, 446 U.S. 680, 697 (1980).

In determining to accept the Offer, the Commission has considered these undertakings.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, it is hereby ORDERED that:

A. Pursuant to Section 8A of the Securities Act and Section 21C of the Exchange Act, Respondent cease and desist from committing or causing any violations and any future violations of Sections 17(a)(2) and 17(a)(3) of the Securities Act, Section 13(a) of the Exchange Act, and Rules 12b-20, 13a-1 and 13a-15(a) thereunder.

B. Respondent shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of $4,000,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. §3717. Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Unisys Corporation as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Jorge Tenreiro, Acting Unit Chief, Crypto Assets and Cyber Unit, Division of Enforcement, Securities and Exchange Commission, 100 Pearl Street, Suite 20-100, New York, NY 10004-261.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil

penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

D. Respondent acknowledges that the Commission is not imposing a civil penalty in excess of $4,000,000 based upon its agreement to cooperate in a Commission investigation or related enforcement action. If at any time following the entry of the Order, the Division of Enforcement ("Division") obtains information indicating that Respondent knowingly provided materially false or misleading information or materials to the Commission, or in a related proceeding, the Division may, at its sole discretion and with prior notice to the Respondent, petition the Commission to reopen this matter and seek an order directing that the Respondent pay an additional civil penalty, Respondent may contest by way of defense in any resulting administrative proceeding whether it knowingly provided materially false or misleading information, but may not: (1) contest the findings in the Order; or (2) assert any defense to liability or remedy, including, but not limited to, any statute of limitations defense.

By the Commission.

Vanessa A. Countryman
Secretary