Substitute Notice of Data Breach

Veolia WTS USA, Inc. fka Suez WTS USA, Inc. fka GE Betz, Inc., and its affiliates and subsidiaries
3600 Horizon Boulevard
Trevose, PA 19053

August 2, 2024

RE: Important Security Notification. Please read this entire letter.

Dear Valued Employee:

We value and respect the privacy of your information, which is why, as a precautionary measure, we are providing this substitute notice to let you know about a cyber security incident that occurred with one of our business associates, the U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA). Veolia was recently notified about a security incident that may affect the security of your personal information. This letter, along with the supplemental letter from CISA, will provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? From January 23, 2024 to January 26, 2024 CISA identified potentially malicious activity, affecting the CSAT Ivanti Connect Secure appliance. CISA immediately took the system offline, isolated the application from the rest of the network, and began a forensic investigation. We are providing this substitute notice because (1) a chemical facility where you had access to restricted areas and/or critical assets may have submitted personally identifiable information (PII) on you for vetting under the Personnel Surety Program or (2) you or a chemical facility submitted limited PII and business contact information for the creation of a CVI Authorized User account between the dates of June 2007 and July 2023.

What Information Was Involved? While CISA's investigation found no evidence of exfiltration of this data, they notified all individuals who had PII submitted to CISA's Chemical Facility Anti-Terrorism Standards (CFATS) program for vetting out of an abundance of caution that this information could have been inappropriately accessed. The information subject to the incident may have included PII submitted through the Personnel Surety Program, which included an individual's name, date of birth, citizenship, or gender. Additional PII was provided, if available or required for a non-U.S. person, including:

- Aliases
- Place of birth
- Citizenship
- Passport Number
- Redress Number
- A Number
- Global Entry ID Number TWIC ID Number

CSAT users who submitted or were involved in the development of Top-Screen surveys, Security Vulnerability Assessments, Site Security Plans (to include CVI authorized users), and CSAT users who submitted personnel surety information may have submitted PII such as name, title, business address, and business phone number. Please note that Veolia submitted PII as part of this program, so you are receiving this notification because your personal information may have been exposed.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Upon learning of the incident, Veolia took immediate measures to deploy additional security procedures to prevent future incidents, as well as engaged cyber security experts to guide us through the incident, ensuring that we fully comply with our legal obligations and properly mitigate the potential impact of the incident.

Veolia will continue to work with cyber security experts and law enforcement to ensure that this incident is properly addressed, ensure that we remain vigilant in the security of our own operations, and continue to strengthen our internal and external controls and safeguards to ensure this type of incident does not occur again. Veolia will notify you of any significant developments that may further impact the security of your personal information.

What Actions You Can Take?
While the investigation found no evidence of credentials being stolen, we would advise you to read and follow CISA's guidance on how to protect yourself from Brute Force Attacks Conducted by Cyber Actors (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), Choosing and Protecting Passwords (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), and Multi-Factor Authentication (https://www.cisa.gov/MFA).
As always, we recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to the appropriate service provider.

We recommend that you obtain, and monitor, your credit reports to ensure that fraudulent activity has not occurred. In line with your rights pursuant to the federal Fair Credit Reporting Act, you may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, by calling toll-free 1 (877) 322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

Additionally, you should report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (1 (877) 438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general can be found here: https://www.naag.org/find-my-ag/

Please take advantage of additional free resources on identity theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacyidentity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Placing a Security Freeze

Certain state law allows consumers to place a security freeze on their credit reports, free of charge. However, a consumer reporting agency may impose a reasonable charge on a consumer for the disclosure of information pertaining to the consumer, for placing a security freeze on a consumer file, temporarily lifting a security freeze for a designated period or for an identified requester, or removing a security freeze, but may not charge a fee in excess of $10. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. We recommend that you work collaboratively with potential lenders, employers and service providers to ensure that you are protecting both your information and the approval status of your applicable request.

In order to place a security freeze on your credit reports, you must contact all three bureaus. You can make your request to place a security freeze to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) via secure email connection provided by each consumer reporting agency. Additionally, your request to place a security freeze may be in the form of a written request, and sent by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872

The credit reporting agencies have five (5) business days after receiving your request to place a security freeze on your credit report, so we recommend placing the freeze as soon as you possibly can. The credit bureaus must also send written confirmation to you within ten (10) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

Lifting or Suspending a Security Freeze

To temporarily lift or suspend the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail (or through each credit reporting agency's secure email connection) and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities, or for the specified period of time.

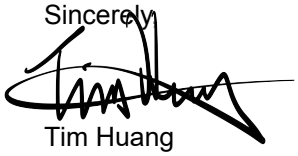
Removing a Security Freeze

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail (or through each credit reporting agency's secure email connection) and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 1(855) 941-5659 Monday through Friday from 8 am – 5:30 pm Central (excluding major U.S. holidays).

Thank you for your immediate attention to this situation, as well as your understanding in the short-term. Our cyber security, as well as the safety and stability of our employees, is of the utmost importance to us and we remain committed to protecting your information. Again, we sincerely apologize for any impact caused by this incident. We will continue to monitor the incident and advise you of any updates as may be necessary.

Sincerely,



Tim Huang
Chief Executive Officer
Veolia WTS USA, Inc. fka Suez WTS USA, Inc. fka GE Betz, Inc., and its affiliates and subsidiaries

VEOLIA

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Privacy, Access, Civil Liberties, and Transparency
Washington, DC 20528

June 20, 2024

Dear Colleague,

As you may know, the Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Security Assessment Tool (CSAT) was the target of a cybersecurity intrusion by a malicious actor from January 23, 2024 to January 26, 2024, which resulted in the potential unauthorized access of Personnel Surety Program submissions and accounts for Authorized Users of Chemical-terrorism Vulnerability Information (CVI).

While CISA's investigation found no evidence of exfiltration of this data, we are notifying all individuals who had their personally identifiable information (PII) submitted to CISA's Chemical Facility Anti-Terrorism Standards (CFATS) program for vetting or had a CVI Authorized User account out of an abundance of caution that this information could have been inappropriately accessed. I share your concern and frustration and am providing you with information we know about this attempted intrusion.

You are receiving this notification because (1) a chemical facility where you had access to restricted areas and/or critical assets may have submitted PII on you for vetting under the Personnel Surety Program or (2) you or a chemical facility submitted limited PII and business contact information for the creation of a CVI Authorized User account between the dates of June 2007 and July 2023. We have also reached out to the chemical facility that you are associated with regarding technical details about the intrusion.

Information Potentially Impacted

Personnel Surety Program. The CFATS Personnel Surety Program enabled CFATS-regulated facilities to comply with Risk-Based Performance Standard (RBPS) 12(iv) —Personnel Surety. RBPS 12(iv)[1] required facility personnel and unescorted visitors who had or were seeking access to restricted areas and critical assets at high-risk chemical facilities to be screened for potential terrorist ties. This included submitting PII through CSAT for direct vetting or repurposing vetting conducted under other Department of Homeland Security programs in order to vet individuals against the Terrorist Screening Database[2].

PII submitted through the Personnel Surety Program included an individual's name, date of birth, citizenship, or gender. Additional PII was provided, if available or required for a non-U.S. person, including:

- Aliases
- Place of Birth

[1] 6 C.F.R. 27.230(a)(12(iv).
[2] For more on the Terrorist Screening Database, visit: https://www.fbi.gov/investigate/terrorism/tsc

- Citizenship
- Passport Number
- Redress Number
- A Number
- Global Entry ID Number
- TWIC ID Number

CSAT User Accounts. In general, there are two types of user accounts for facilities submitting information for CSAT: CSAT users submitting or involved in the development of Top-Screen surveys, Security Vulnerability Assessments, and Site Security Plans (to include CVI authorized users) and CSAT users submitting personnel surety information. In both cases, the information collected for the creation of a CSAT account is the same: name, title, business address, and business phone number.

Details of the Intrusion

On January 26, CISA identified potentially malicious activity[3] affecting the CSAT Ivanti Connect Secure appliance. CISA immediately took the system offline, isolated the application from the rest of the network, and began a forensic investigation. This investigation included technical experts from CISA's Office of the Chief Information Officer, our Cybersecurity Division's Threat Hunting team, and the Department of Homeland Security's Network Operations Center.

During the investigation, we identified that a malicious actor installed an advanced webshell on the Ivanti device. This type of webshell can be used to execute malicious commands or write files to the underlying system. Our analysis further identified that a malicious actor accessed the webshell several times over a two-day period.

Importantly, the investigation has concluded and did not identify exfiltration of data from CSAT or adversary access beyond the Ivanti device. All information in CSAT was encrypted using AES 256 encryption and information from each application had additional security controls limiting the likelihood of lateral access. Encryption keys were hidden from the type of access the threat actor had to the system.

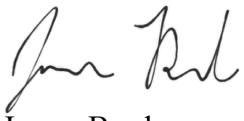
Recommendations for Impacted Individuals

While the investigation found no evidence of credentials being stolen, we would advise you to read and follow CISA's guidance on how to protect yourself from Brute Force Attacks Conducted by Cyber Actors (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), Choosing and Protecting Passwords (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), and Multi-Factor Authentication (https://www.cisa.gov/MFA).

[3] For more on this type of malicious activity, visit: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

CISA has created a website with copies of this notice, frequently asked questions, periodic updates, and an opportunity to sign up for an email distribution list to receive updates on the website. As CISA explores additional possible remediations, we encourage you to sign up to our distribution list for this incident to receive all the latest updates at www.cisa.gov/csat-notification. Questions about this incident by impacted individuals should be addressed to the CISA Chemical Security Subdivision at CFATS.Notificiations@cisa.dhs.gov.

Sincerely,



James Burd
Chief Privacy Officer

Sprechen Sie kein Englisch? Bitte besuchen Sie www.cisa.gov/csat-notification und wählen Sie Ihre bevorzugte Sprache für diesen Brief.

Sprechen Sie kein Englisch? Bitte besuchen Sie www.cisa.gov/csat-notification und wählen Sie Ihre bevorzugte Sprache für diesen Brief.

انگلیسی صحبت نمی کنید؟ لطفاً از www.cisa.gov/csat-notification دیدن کنید و زبان مورد نظر خود را برای این نامه انتخاب کنید.

Vous ne parlez pas anglais ? Veuillez visiter www.cisa.gov/csat-notification et choisir votre langue préférée pour cette lettre.

अंग्रेज़ी नहीं बोलते हैं? कृपया www.cisa.gov/csat-notification पर जाएँ और इस पत्र के लिए अपनी पसंदीदा भाषा को चुनें।

英語以外の言語で本通知を確認する場合は、www.cisa.gov/csat-notification をより、希望の言語を選択してください。

영어를 사용하지 않습니까? www.cisa.gov/csat-notification 을 방문하여 이 편지에 대해 원하는 언어를 선택하세요.

Hindi nakakapagsalita ng Ingles? Mangyaring bumisita sa www.cisa.gov/csat-notification at piliin ang mas gusto mong wika para sa liham na ito.

不懂英语？请访问 www.cisa.gov/csat-notification ， 选择您喜欢的语言来阅读这封信。

不懂英語？請訪問 www.cisa.gov/csat-notification 選擇您喜歡的語言來閱讀這封信。