



June 20, 2024

Dear Stakeholders,

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. While CISA's investigation found no evidence of exfiltration of data, this may have resulted in the potential unauthorized access of Top-Screen surveys, Security Vulnerability Assessments, Site Security Plans, Personnel Surety Program submissions, and CSAT user accounts. Thus, we are notifying all impacted participants of the Chemical Facility Anti-Terrorism Standards (CFATS) program 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 your company may have submitted Top-Screen surveys, Security Vulnerability Assessments (SVA), or Site Security Plans (SSP) to the CFATS program via CSAT; submitted personally identifiable information (PII) of your employees, visitors, or other third parties for vetting under the Personnel Surety Program; or submitted limited PII and business contact information to access Chemical-terrorism Vulnerability Information (CVI) or for the creation of a CSAT account between June 2007 and July 2023.

We are providing this notification to present mutually beneficial and voluntary options that may mitigate the impacts to relevant persons for whom you have contact information in your records and files.

Information Potentially Impacted

Top-Screen Surveys. Facilities that possess any chemical of interest¹ at or above the specified screening threshold quantity and concentration were considered chemical facilities of interest under the CFATS program and were required to report their chemical holdings to CISA by filling out a Top-Screen survey. Top-Screen surveys included information about facility topography, types of chemicals of interest at the facility, and characteristics of those chemicals and their storage.

Security Vulnerability Assessments. All covered chemical facilities were required to complete an SVA to identify the facility's use of chemicals of interest, critical assets², and measures related to the facility's policies, procedures, and resources that are necessary to support

¹ For more information on chemicals of interest, visit: <https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/appendix-chemicals-interest>

² For more information on what is a critical asset, visit: <https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/chemical-security-assessment-tool-csat/security-vulnerability-assessment-and-site-security-plan>

the facility's security plan. The SVA allowed the facility to provide an analysis of the facility's security posture and potential vulnerabilities which may have included incomplete documentation, lack of training, or insufficient resources.

Site Security Plans and Alternative Security Programs (ASP). Along with the SVA, all covered chemical facilities were required to submit an SSP, or ASP in lieu of an SSP, to describe existing or planned security measures required to meet the CFATS Risk-Based Performance Standards³ (RBPS).

Personnel Surety Program. The CFATS Personnel Surety Program enabled CFATS-regulated facilities to comply with RBPS 12(iv),⁴ which 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 Database⁵. The minimum PII elements provided for a U.S. Person included an individual's name, date of birth, and 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 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, SVAs, and SSPs (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 activity⁶ 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

³ 6 C.F.R. 27.230(a). For more information on Risk-Based Performance Standards, visit:

<https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-risk-based-performance-standards>

⁴ 6 C.F.R. 27.230(a)(12)(iv).

⁵ For more on the Terrorist Screening Database, visit: <https://www.fbi.gov/investigate/terrorism/tsc>

⁶ For more on this type of malicious activity, visit: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>

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, our investigation has concluded and did not identify adversarial access beyond the Ivanti device nor data exfiltration from the CSAT environment. 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 Facility Action

CISA encourages facilities to maintain cybersecurity and physical security measures and address vulnerabilities, both physical and virtual, according to their normal procedures. While the investigation found no evidence of credentials being stolen, CISA encourages individuals who had CSAT accounts to reset the passwords for any account, business or personal, which used the same password. This can help to prevent possible "password spraying" attacks⁷ in the future.

Voluntary Notification Options

CISA was not authorized to, and did not collect, the address or contact information for individuals vetted under the Personnel Surety Program. As a result, CISA is unable to directly contact those individuals who had their information submitted by chemical facilities for terrorist vetting.

As such, we request that you, on a voluntary basis, notify those individuals for whom you have contact information of this incident. CISA is willing to provide a template notice for your use in that effort. Alternatively, should you decline to notify those individuals, we request that you, also on a voluntary basis, provide CISA with the contact information currently maintained in your files of relevant persons impacted by this incident so it can directly notify impacted individuals. We can coordinate on receiving such information securely. Again, CISA emphasizes that your decision to take either action is voluntary and may be declined at your facility's discretion. Furthermore, your participation will be without compensation or opportunity to file a claim.

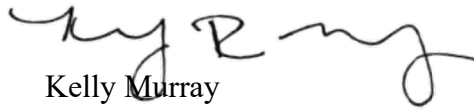
In addition to potential direct notification to impacted individuals, CISA will also establish a public website notifying potentially impacted individuals of the incident. CISA will

⁷ For more information on "password spraying," visit: <https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors#:~:text=During%20a%20password%20spray%20attack,rapid%20or%20frequent%20account%20lockouts>

include on its website copies of this notice in multiple languages, frequently asked questions, notices for industry webinars, and remediation instructions for impacted individuals at www.cisa.gov/cfats-incident.

In closing, while CISA's investigation did not result in any evidence of exfiltration of data or lateral movement, we are notifying all potentially impacted facilities out of the abundance of caution that this information could have been inappropriately accessed. Questions about this incident by chemical facilities or their third-party partners should be addressed to the CISA Chemical Security Subdivision at CFATS.Notifications@cisa.dhs.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Kelly Murray". The signature is fluid and cursive, with a large initial "K" and "M".

Kelly Murray
Associate Director