

LINDSEY O. GRAHAM, SOUTH CAROLINA  
 JOHN CORNYN, TEXAS  
 MICHAEL S. LEE, UTAH  
 TED CRUZ, TEXAS  
 JOSH HAWLEY, MISSOURI  
 THOM TILLIS, NORTH CAROLINA  
 JOHN KENNEDY, LOUISIANA  
 MARSHA BLACKBURN, TENNESSEE  
 ERIC SCHMITT, MISSOURI  
 KATIE BOYD BRITT, ALABAMA  
 ASHLEY MOODY, FLORIDA

RICHARD J. DURBIN, ILLINOIS  
 SHELDON WHITEHOUSE, RHODE ISLAND  
 AMY KLOBUCHAR, MINNESOTA  
 CHRISTOPHER A. COONS, DELAWARE  
 RICHARD BLUMENTHAL, CONNECTICUT  
 MAZIE HIRONO, HAWAII  
 CORY A. BOOKER, NEW JERSEY  
 ALEX PADILLA, CALIFORNIA  
 PETER WELCH, VERMONT  
 ADAM B. SCHIFF, CALIFORNIA

# United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

March 11, 2025

## VIA ELECTRONIC TRANSMISSION

Ms. Bridget Bean  
 Executive Director  
 Cybersecurity and Infrastructure Security Agency

Dear Executive Director Bean:

On July 3, 2024, I sent then-Director of the Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, a letter requesting information regarding potential malicious activity that affected CISA's Chemical Security Assessment Tool (CSAT) Ivanti Connect Secure appliance.<sup>1</sup> I also raised concerns and asked questions related to reporting that CISA's Infrastructure Protection (IP) Gateway, now known as CISA Gateway, was breached, which would potentially expose critical information about the operations of U.S. critical infrastructure.<sup>2</sup> On August 1, 2024, then-Director Easterly responded to my letter, but the response failed to fully and completely answer the questions raised in my July 3 letter, as well as failed to provide all responsive records.<sup>3</sup> Specifically, CISA's response failed to answer questions 1, 2, 8, and 9.<sup>4</sup> CISA partially answered questions 3, 4, and 7.<sup>5</sup> The information CISA did provide raises additional concerns and questions related to the January 23-26, 2024, intrusion.<sup>6</sup>

The response stated that CISA was monitoring vulnerabilities related to Ivanti and the Ivanti Pulse Secure Appliance in "early January 2024," and issued an Emergency Directive on January 19 to "federal agencies in order to protect federal networks from a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the cybersecurity of an agency."<sup>7</sup> However, it is unclear from the response when CISA first discovered the vulnerabilities and how CISA protected itself and other agencies, beyond compliance with the emergency directive, from the threat.<sup>8</sup> Further, the former Director's response mentioned that CISA provided "written formal notification" to impacted entities, and that CISA "conducted its own assessment utilizing the National Institute of Standards and Technology (NIST) Risk Management Framework and NIST 800 series controls."<sup>9</sup> Yet to date, CISA has failed to provide these records, which I requested.

<sup>1</sup> Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity & Infrastructure Security Agency (July 3, 2024), [https://www.grassley.senate.gov/imo/media/doc/grassley\\_to\\_cisa\\_-\\_cyberattack.pdf](https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf).

<sup>2</sup> *Id.*; Jonathan Greig and Suzanne Smalley, *CISA forced to take two systems offline last month after Ivanti compromise* (Mar. 8, 2024), The Record, <https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise>; Julie Pattison-Gordon, *Federal Cyber Agency Offlines 2 Systems After Ivanti Hack* (Mar. 13, 2024), Government Technology, <https://www.govtech.com/security/federal-cyber-agency-offlines-2-systems-after-ivanti-hack>.

<sup>3</sup> Letter from the Honorable Jen Easterly, Director, Cybersecurity & Infrastructure Security Agency, to Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee (Aug. 1, 2024), Exhibit 1; Department of Homeland Security, *Supplemental Notice to Congress of an Incident Under Section 3554(b)(7)(C)(iii)(III)(bb) of the Federal Information Security Modernization Act of 2014* (Apr. 21, 2024), Exhibit 2.

<sup>4</sup> Exhibit 1, *supra* note 3.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*; CISA, *Chemical Security Assessment Tool (CSAT) Ivanti Notification*, <https://www.cisa.gov/chemical-security-assessment-tool-csat-ivanti-notification>.

<sup>7</sup> Exhibit 1, *supra* note 3.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

Additionally, the Department of Homeland Security's (DHS) *Supplemental Notice to Congress of an Incident Under Section 3554(b)(7)(C)(iii)(III)(bb) of the Federal Information Security Modernization Act of 2014* also raises additional concerns and questions.<sup>10</sup> For instance, the notice states that at the time the Congressional notice was sent, forensic analysis of the incident was ongoing, and CISA had "open[ed] line of communication among all related parties to share analysis findings, indicators of compromise (IOCs), and tactics, techniques, and procedures (TTPs) to better understand the adversary."<sup>11</sup> To date, I have yet to receive the results of this forensic analysis or these communications with stakeholders, which I requested in my July 2024 letter. The notice also highlighted that the CSAT tool "contains many datasets, including the results of Top-Screen surveys, Security Vulnerability Assessments and Site Security Plans, and Personnel Surety vetting submission information. While much of this information may be publicly available via different websites and public sources, the Personnel Surety Program data generally is not."<sup>12</sup> According to the notice, the Personnel Surety Program contains personally identifiable information (PII) on 506,191 individuals, which was submitted by chemical facilities and companies that were subject to the Chemical Facility Anti-Terrorism Standards (CFATS) program.<sup>13</sup> The collection of this PII, according to the notice, was used to assist "CFATS vetting requirements for the individuals who sought access to a chemical facility high-risk area through July 2023."<sup>14</sup>

According to the Congressional notice, DHS and CISA deemed this threat to be "moderate," despite the threat actor having access to the CSAT environment for two days.<sup>15</sup> In regards to the unauthorized access to the data, the response said, "CISA cannot disprove access or exfiltration with a high degree of confidence. Further, CISA does not have knowledge or evidence of misuse of the PII, nor can it definitively speak to any related criminal activity or who may have received compromised PII if it was exfiltrated."<sup>16</sup> It appears that CISA cannot definitively determine whether or not the data on 506,191 individuals has been misused, exfiltrated, or used in furtherance of criminal activity.<sup>17</sup> According to the notice, as of April 21, 2024, a threat actor still had not been identified.<sup>18</sup> These are questions that CISA, whose mission is to "lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure," should be able to answer.<sup>19</sup> Accordingly, I'm requesting a status update on this matter.

So that Congress can conduct independent oversight of CISA and its handling of the January 23-26, 2024, intrusion, please provide answers to the following questions by March 25, 2025:

1. Provide a full and complete response, including all responsive records, to my July 3, 2024, letter.

---

<sup>10</sup> Exhibit 2, *supra* note 3.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* ("The dataset included combinations of individuals' names, aliases, dates of birth, gender, places of birth, citizenship, passport numbers, A-numbers, Trusted Traveler credential numbers, and Transportation Worker Identification Card (TWIC) numbers, in some cases, for vetting against various screening databases, including the Terrorist Screening Database (TSDB).").

<sup>14</sup> *Id.* ("Every record of an individual contained the full name and date of birth of the individual, and nearly all records contained the individual's gender. Less than half of the records contained an individual's citizenship, and less than 6% contained a city, state, country, or country of birth. Less than 1% of records contained other PII.").

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> CISA, *About CISA*, <https://www.cisa.gov/about>.

2. Provide all Congressional notifications regarding the January 2024 intrusion.
3. When exactly did CISA discover the Ivanti vulnerabilities? What specific steps did CISA take to secure all systems, including the CSAT tool, using Ivanti products? How many systems at CISA are currently using Ivanti tools and products? Provide all records.<sup>20</sup>
4. How many assessments, audits, or investigations has CISA completed related to the January 2024 intrusion? Provide copies of all findings.
5. Has CISA completed all forensic analysis related to the January 2024 intrusion? If not, why not? If yes, provide copies of all reports and findings.
6. Provide copies all formal written notifications to affected individuals, organizations, and entities.
7. Provide all communications with “related parties” and stakeholders with respect to the January 2024 intrusion.
8. Did the threat actor exfiltrate any of the Personnel Surety Program data? If so, what kind of data and how much was exfiltrated? Provide all records.
9. How does CISA develop its threat assessments? Provide a copy of the threat assessment related to the January 2024 intrusion.

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-5225.

Sincerely,



Charles E. Grassley  
Chairman  
Committee on the Judiciary

---

<sup>20</sup> “Records” include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (e-mails, email attachments, and any other electronically-created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

# EXHIBIT 1



U.S. Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency  
Office of the Director  
Washington, DC 20528

August 1, 2024

The Honorable Charles E. Grassley  
Ranking Member  
Committee on the Budget  
United States Senate  
Washington, DC 20510

Dear Senator Grassley:

Thank you for your July 3, 2024, letter.

The Cybersecurity and Infrastructure Security Agency (CISA) monitored Ivanti and open-source reporting related to vulnerabilities within the Ivanti Pulse Secure Appliance (Virtual Private Network (VPN) solution) in early January 2024. On January 19, CISA issued *Emergency Directive 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*, a compulsory directive from CISA to federal agencies in order to protect federal networks from a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the cybersecurity of an agency. CISA rapidly complied with this emergency directive for its own systems including the systems impacted by the incident you reference, which is described below.

On January 25 and 26, 2024, CISA received information from a security researcher and a CISA vendor regarding Ivanti vulnerabilities enabling compromises of two information technology systems: CISA Gateway and the Chemical Security Assessment Tool (CSAT). Once credible indicators of compromise (IOCs) were observed, CISA immediately initiated incident response activities. These efforts greatly reduced exposure and interrupted the actor's ability to exfiltrate data from the systems. To date, CISA has not seen any indications of records being inappropriately accessed or exfiltrated from either system. However, out of an abundance of caution, the Department of Homeland Security (DHS) determined that this incident involved systems containing personally identifiable information and met the definition of a "major incident" as defined in Office of Management and Budget (OMB) Memorandum M-24-04 triggering the notification requirements of the Federal Information Security Modernization Act (FISMA) (44 U.S.C. 3554(b)(7)(C)(iii)(III)). In accordance with FISMA, DHS provided written notifications of the major incident to the statutorily mandated Congressional committees. CISA also offered multiple briefings to its committees of jurisdiction regarding the incident.

The most recent notification to Congressional committees is enclosed, which addresses many of the questions raised in your letter. CISA provided briefings on the incident to organizations representing impacted entities, such as the Chemical Sector Coordinating Council (SCC) and written formal notification of the incident to impacted entities. Prior to operating the systems, CISA conducted its own assessment utilizing the National Institute of Standards and Technology (NIST) Risk Management Framework and NIST 800 series controls, resulting in an authorization to operate the systems.

The Honorable Charles E. Grassley  
Page 2

Thank you again for your letter. Should you need additional assistance, please have your staff contact the Office of Legislative Affairs at [CISA\\_OLA@cisa.dhs.gov](mailto:CISA_OLA@cisa.dhs.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "Jen Easterly", with a stylized flourish at the end.

Jen Easterly  
Director

Enclosure

**EXHIBIT 2**  
FOR OFFICIAL USE ONLY

Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

April 21, 2024

Pursuant to the requirements of Title 44 of U.S. Code Section 3554(b)(7)(C)(iii)(III)(bb) of the *Federal Information Security Modernization Act of 2014* (FISMA), the U.S. Department of Homeland Security (DHS) is submitting the enclosed notice to the following Members of Congress:

The Honorable Patty Murray  
Chair, Senate Committee on Appropriations

The Honorable Susan M. Collins  
Vice Chair, Senate Committee on Appropriations

The Honorable Gary C. Peters  
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rand Paul  
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Maria Cantwell  
Chair, Senate Committee on Commerce, Science, and Transportation

The Honorable Ted Cruz  
Ranking Member, Senate Committee on Commerce, Science, and Transportation

The Honorable Tom Cole  
Chairman, House Committee on Appropriations

The Honorable Rosa DeLauro  
Ranking Member, House Committee on Appropriations

The Honorable Mark E. Green  
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson  
Ranking Member, House Committee on Homeland Security

The Honorable James Comer  
Chairman, House Committee on Oversight and Accountability

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

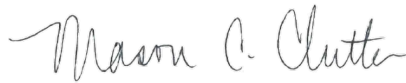
The Honorable Jamie Raskin  
Ranking Member, House Committee on Oversight and Accountability

The Honorable Frank D. Lucas  
Chairman, House Committee on Science, Space, and Technology

The Honorable Zoe Lofgren  
Ranking Member, House Committee on Science, Space, and Technology

Should you have any questions or comments, please contact the DHS Office of Legislative Affairs at (202) 447-5890.

Sincerely,



Mason Clutter  
Chief Privacy Officer



RADM Chris Bartz  
Deputy Chief Information Officer

on behalf of Eric Hysen  
Chief Information Officer

FOR OFFICIAL USE ONLY

---

**Department of Homeland Security  
(DHS)**

**Supplemental Notice to Congress of an Incident Under Section 3554(b)(7)(C)(iii)(III)(bb) of the  
Federal Information Security Modernization Act of 2014**

On March 29, 2024, DHS submitted to the congressional committees listed in the enclosed transmittal letter (“congressional committees”) a seven-day notice of a cybersecurity incident with privacy implications constituting a “major incident” as required under FISMA.<sup>1</sup>

FISMA further requires agencies to provide designated congressional committees a summary describing additional information relating to the incident “within a reasonable period of time after additional information relating to the incident is discovered.”<sup>2</sup> The Office of Management and Budget (OMB) guidance states that agencies must supplement their initial seven-day notice to the congressional committees with a report no later than 30 days after the agency discovers the “major incident.”<sup>3</sup>

The following supplemental report is being provided pursuant to these requirements. The report is based on information currently available to DHS and reflects the ongoing mitigation steps being taken to address the incident.

---

<sup>1</sup> 44 U.S.C. § 3554(b)(7)(C)(iii)(III)(aa).

<sup>2</sup> 44 U.S.C. § 3554(b)(7)(C)(iii)(III)(bb). This information includes a summary of the threats and threat actors, vulnerabilities, and impacts relating to the incident; the risk assessments conducted under Section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred; the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and the detection, response, and remediation actions. 44 U.S.C. § 3554(c)(1)(A)(i)(I)-(IV).

<sup>3</sup> OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements* (Nov. 19, 2019), *available at*: The supplemental report must include a summary of information available about the breach, including how the breach occurred, based on information available to agency officials on the date which the agency submits the report; an estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals; a description of any circumstances necessitating a delay in providing notice to affected individuals; and an estimate of whether and when the agency will provide notice to affected individuals. See also 44 U.S.C. § 3553, note “Breaches,” (Pub. L. 113–283, §2(d), Dec. 18, 2014, 128 Stat. 3085).



---

## *I. Background*

On January 26, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) received credible information from a reputable CISA vendor indicating that the Chemical Security Assessment Tool (CSAT) system was possibly compromised by an unknown threat actor via zero-day vulnerabilities present in the newly released Ivanti Connect Secure. CISA and DHS immediately initiated incident response procedures and successfully isolated the CSAT system from the network. Forensic analysis was performed on the impacted devices, and initial analysis found evidence of compromise on or around January 25<sup>th</sup>, 2024. Forensic analysis is still ongoing.

In addition to incident response and isolation procedures, CISA developed an open line of communication among all related parties to share analysis findings, indicators of compromise (IOCs)<sup>1</sup>, and tactics, techniques, and procedures (TTPs)<sup>2</sup> to better understand the adversary.

On March 25, 2024, DHS determined that this incident involved personally identifiable information (PII) and met the definition of a “major incident” as defined in OMB Memorandum M-24-04, thus triggering the notification requirements pursuant to Section 3554(b)(7)(C)(iii)(III) of the FISMA.

## *II. Supplemental Report Update*

On March 28, 2024, the DHS Chief Privacy Officer convened the privacy Breach Response Team in accordance with OMB guidance<sup>3</sup> and DHS policy<sup>4</sup> to assess the privacy incident and discuss appropriate mitigation and remediation measures.

CSAT contains many datasets, including the results of Top-Screen surveys<sup>5</sup>, Security Vulnerability Assessments and Site Security Plans, and Personnel Surety vetting submission information. While much of this information may be publicly available via different websites and public sources, the Personnel Surety Program data generally is not.

The Personnel Surety Program is the primary dataset in CSAT containing PII on 506,191 unique individuals. Chemical facilities and companies subject to the Chemical Facility Anti-Terrorism Standards (CFATS) program submitted the PII maintained in CSAT to CISA. The PII collection occurred and supported CFATS vetting requirements for the individuals who sought access to a chemical facility high-risk area through July 2023. The CFATS vetting typically was a term of employment. The dataset included combinations of individuals’ names, aliases, dates of birth, gender, places of birth, citizenship, passport numbers, A-numbers, Trusted Traveler credential numbers, and Transportation Worker Identification Card (TWIC) numbers, in some cases, for vetting against various

---

<sup>1</sup> IOCs are digital and informational “clues” that incident responders use to detect, diagnose, halt, and remediate malicious activity in their networks.

<sup>2</sup> TTPs, in this context, are descriptions of the adversary’s behavior. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.

<sup>3</sup> Office of Management and Budget Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).

<sup>4</sup> DHS Directive 047-01-006, PRIVACY INCIDENT RESPONSIBILITIES AND BREACH RESPONSE TEAM, (December 4, 2017) requires the Breach Response Team be convened within 72 hours of first being notified of a major privacy incident.

<sup>5</sup> Under the Chemical Facilities Anti-Terrorism Standards program, facilities that possess any chemicals of interest at or above the specified screening threshold quantities and concentration were required to report their chemical holdings to CISA by filling out a Top-Screen survey.

screening databases, including the Terrorist Screening Database (TSDB).

Every record of an individual contained the full name and date of birth of the individual, and nearly all records contained the individual's gender. Less than half of the records contained an individual's citizenship, and less than 6% contained a city, state, country, or country of birth. Less than 1% of records contained other PII.

The impacted system was taken offline and removed from the network. Forensics analysis as part of the "Containment, Eradication & Recovery," as outlined in NIST 800-61, "Computer Security Incident Handling Guide," is still ongoing. As new TTPs and IOCs are discovered, they are shared through the appropriate channels.

### *III. Assessment of Risk*

The privacy Breach Response Team determined this privacy incident presents a moderate risk of harm to the individuals potentially impacted by the incident.

While the threat actor appears to have had access to the CSAT environment for two days, CISA does not have evidence of lateral movement, exfiltration of the data, or access to encryption keys. However, due to the limited visibility within the antiquated CSAT, CISA cannot disprove access or exfiltration with a high degree of confidence. Further, CISA does not have knowledge or evidence of misuse of the PII, nor can it definitively speak to any related criminal activity or who may have received compromised PII if it was exfiltrated.

CISA encrypted the PII at rest in CSAT using AES 256 encryption. While CISA discovered copies of the encryption keys stored within the CSAT environment, CISA reports that the system architecture would have made those keys invisible to the threat actors. Additionally, CISA employed additional access controls between applications within CSAT.

While CISA has not yet made positive attribution to a specific threat actor, the tactics used by the threat actor were consistent with CISA advisories<sup>6</sup> concerning state-sponsored actors and Ivanti virtual private network (VPN) appliances.

CISA is working with the Department to notify potentially impacted individuals of this incident through direct notification, and substitute notification on the CISA website, providing information about the incident along with contact information.

---

<sup>6</sup> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>