CYBERSECURITY INCIDENTS

This guidance explains the process and roles and responsibilities of U.S. Customs and Border Protection (CBP) and the brokerage community on how to facilitate, to the extent possible, the importation, entry, and entry summary process, in the event of a cybersecurity incident affecting a broker. This guidance is a supplement to the one-page Cyber Incident Guidance for Customs Brokers published in March 2023 on CBP.gov. CBP will authorize downtime procedures and enforcement discretion as appropriate and needed, subject to CBP discretion, on a case-by-case basis.

Definitions

- Downtime – For purposes of this document, downtime refers to the alternative cargo release process described herein, which is authorized based on a determination by the Office of Field Operations (OFO) when a demonstrated cybersecurity incident prevents a broker from electronically filing in the Automated Commercial Environment (ACE), the "entry" documentation and information required by 19 C.F.R. § 142.3 to secure **cargo release** from customs custody on behalf of the broker's clients. If downtime is authorized, the affected broker must submit a "downtime letter" and supporting documentation (including, but not limited to, the invoice and completed CBP Form 3461) by email to a designated CBP official to temporarily provide the requisite entry documentation and information outside of ACE. For this limited downtime purpose, this email submission will serve as a "CBP-authorized electronic data interchange system" to file entry documentation and information. Partner Government Agency (PGA) admissibility requirements still apply to shipments that CBP releases on downtime, and CBP cannot release a shipment without the necessary PGA approval. Once the broker's system is fully up and running after the cybersecurity incident, as defined below, the broker is required to electronically file in ACE all entries released through downtime processing. Please note, the entry filing deadlines are not affected/waived by the authorization of any downtime.

- Enforcement Discretion – For purposes of this guidance, CBP may work with a broker who is the victim of a cybersecurity incident to provide discretion to the extent possible for post-release transactions.

- Fully up and running – For purposes of this document, fully up and running system status refers to a determination by CBP's Office of Information and Technology (OIT) that, from a security standpoint, it is safe and secure for a broker affected by a demonstrated cybersecurity incident to reconnect to ACE and that the broker's systems are sufficiently restored to permit the transmission of entry and entry summary documentation and information to CBP through the Automated Broker Interface (ABI)/ACE. Such a determination cannot be made until the broker has taken the necessary steps to review patterns in technical processing, conducted human investigations of the cybersecurity incident, etc.

Reporting a Cybersecurity Incident

1. The broker must report the cybersecurity incident as soon as possible to the CBP OIT Security Operations Center (SOC) at 703-921-6507 or cbpsoc@cbp.dhs.gov. A broker will also report their cybersecurity incident to designated CBP personnel at cyberincident@cbp.dhs.gov.

   Pursuant to 19 C.F.R. § 111.21(b), brokers must also report any known breach of physical or electronic records relating to customs business to the SOC no later than 72 hours after discovery of the breach, including any known compromised importer identification numbers or other personally identifiable information.

   The broker must also provide their Indicators of Compromise to the SOC.

2. OIT's Cargo Systems Program Directorate Information System Security Manager will confirm the broker has an Interconnection Security Agreement on file and ensure that it is up to date.

3. The broker must inform impacted PGAs of their outage to receive admissibility clearance guidance. If needed, CBP's Office of Trade (OT) Headquarters will provide the broker with the appropriate point of contact for the impacted PGAs.

4. CBP is not responsible for and will not notify importers that the special entry or entry summary procedures described herein were employed for any entry filed by a broker who is experiencing a cybersecurity incident. CBP encourages brokers to notify their clients (importers) of the cybersecurity incident. CBP understands that there may be specific factors that the broker considers when or if a client is notified (timeframe of cybersecurity incident, whether the particular client's entries were impacted, etc.). If the broker has notified their clients, they should inform CBP which importers have been notified (e.g., all clients, only clients with time sensitive imports, only clients in certain geographical location, etc.). Brokers who are part of the Customs-Trade Partnership Against Terrorism may use their required notification plan when informing their clients of the cybersecurity incident.

Determination of Risk Surrounding a Cybersecurity Incident

1. When the broker reports the cybersecurity incident to the SOC, they should expect the following questions to be posed (understanding that every answer may not be available at the time of first reporting of the cybersecurity incident, but will be provided immediately once available):

a. What is the root cause of the incident?
b. What is the nature of the cyber intrusion?
c. What are the attack vectors?
d. What systems/applications are impacted?
e. How does the cyber incident impact ACE?
f. Do you have a direct connection to ACE, or do you use a service center?
g. What are the Indicators of Compromise?
h. What is the scale of the outage (local, national, global)?
i. What is the length of the outage (hours, days, weeks)?
j. What mitigation procedures are being performed by the broker?
k. What is the estimated timeline to resolution?
l. Any additional follow-up questions as needed.

2. CBP leadership will determine risk to CBP systems and corresponding actions required, including potentially disconnecting the broker from ACE.

3. Constant and open communication is vital to ensure operations flow as smoothly as possible. CBP Headquarters will schedule regular meetings with the broker, CBP, and impacted PGAs. CBP parties include:
   - OIT SOC;
   - OT Client Representatives;
   - OT Commercial Operations Revenue & Entry Division;
   - OT Interagency Collaboration Division;
   - OT Trade Modernization Division;
   - OT Entry Summary, Accounts and Revenue Division;
   - OT Cargo Control and Release Division;
   - OFO Cargo Security and Control Division;
   - OFO Trade Operations Division; and
   - OFO Customs Trade Partnership Against Terrorism (CTPAT).

4. The broker must also maintain communication on an as-needed basis with the affected ports of entry, Centers of Excellence and Expertise (Centers), and Supply Chain Security Specialist if part of the CTPAT program.

<u>Downtime Process</u>

1. OFO Headquarters (HQ) will determine on a case-by-case basis whether to authorize downtime procedures for the broker.

2. If OFO HQ authorizes downtime, CBP will inform port and Center personnel of the authorized downtime and provide the internal CBP message number to the broker for reference.

3. The broker may be allowed to submit a downtime letter that includes the CBP Form 3461 mandatory and conditional (as necessary) data elements listed below and found in the ACE CATAIR Cargo Release Chapter, to the port for every shipment released on downtime.

   Mandatory: Seller Name and Address, 10 Digit Harmonized Tariff Schedule number, Country of Origin, Bill of Lading/House Air Waybill Number, Entry Number, Entry Type, Estimated Entry Value

   Conditional: Importer of Record Number, Buyer Name and Address, Consignee Number, Manufacturer/Supplier Name and Address, Bill of Lading Issuer Code

   These downtime letters are submitted as a cover letter with all other necessary documents (CBP Form 3461, invoice, bill of lading, PGA documents, etc.) attached in hard copy to the port and via email to cbpdowntimedocs@cbp.dhs.gov. The submission must contain the required information and must be certified by the importer of record or their duly authorized customs broker as being true and correct to the best of their knowledge. Brokers must have a bank of entry numbers, accessible without system access, on hand for downtime requests.

   Certifying statement added to the downtime letter:
   I hereby make application for entry/immediate delivery. I certify that the above information is accurate, the bond is sufficient, valid, and current, and that all requirements of 19 C.F.R. Part 142 have been met.

4. PGAs do not authorize downtime. Paper PGA form submissions and PGA web-based systems (outside of ACE) are required for PGA-impacted goods. The broker is required to directly submit the PGA forms and PGA web-based systems data to the PGA along with a copy of the downtime letter associated to the entry. Downtime will not be authorized for any entry subject to PGA requirements for which PGA approval for release is not obtained.

5. If downtime is authorized, brokers must utilize risk management to determine if downtime processing should be requested for shipments.

6. After OIT determines the broker's system is fully up and running, the

broker is required to transmit via ABI each entry released on downtime to ACE within five business days. The broker must attach the associated downtime letter to each entry in ACE via the Document Image System (DIS).

Enforcement Discretion Process

1. OT HQ and OFO HQ will consider authorizing enforcement discretion for the broker on a case-by-case basis.

2. Post-release transactions that are not included in CBP's consideration for enforcement discretion due to legal deadlines are post-summary corrections, protests, reconciliations for post-import refund claims under 19 U.S.C. §1520(d) (520d reconciliations), and drawback.

3. For all entries impacted by the cybersecurity incident that were **not** released on downtime but for which OT and OFO determined the use of enforcement discretion was authorized, the broker is required to attach a DIS document on the entry summary including the broker, date range of enforcement discretion, and reason for enforcement discretion (cybersecurity incident).

4. The broker must transmit to ACE all post-release transactions immediately once the broker's system is fully up and running.

5. While CBP has some flexibility regarding liquidated damages, the collection of interest is required by statute when estimated duties, taxes, and fees are paid late, pursuant to 19 U.S.C. § 1505 and its implementing regulation at 19 C.F.R. § 24.3a. Interest accrued due to late payment of estimated duties, taxes, and fees incidental to a broker cybersecurity incident may be collected using the following options.

    a. Voluntary Tenders: While under no obligation to do so, impacted brokers may submit a voluntary tender or tenders on behalf of their importer clients to resolve interest debt on entries affected by the cybersecurity incident. The tender amount may be calculated either on an entry-by-entry basis or via use of the midpoint calculation that is used to determine interest payment on an aggregate reconciliation. The payment should designate that it is for additional monies due for interest on entries submitted or transmitted by (BROKER NAME) affected by a cybersecurity incident that commenced on (DD/MM/YY) and concluded on (DD/MM/YY). The payment should be collected on a cash receipt.

    b. Payment of interest other than by voluntary tender: If no voluntary tender is submitted, CBP will collect interest through its usual

administrative processes. Each affected importer of record and its surety will be notified of the unpaid debt and encouraged to pay it. Interest will accrue in accordance with 19 U.S.C. § 1505 and 19 C.F.R. § 24.3a until paid by the import of record or its surety.

Reporting Transactions Impacted by the Cybersecurity Incident

1. The broker will be responsible for identifying the full scope of the entries and/or post-release transactions impacted by the cybersecurity incident.

2. The broker will provide a daily report of every entry released during the approved downtime period to cyberincident@cbp.dhs.gov along with the impacted Port Directors and Center Directors or their designees, with the following cargo release information, with the understanding that "Date input in ACE" will be added immediately once each entry is input into ACE and sent to CBP.

Cargo Release					
Entry Number	Port of Entry (POE)	Released on Downtime? (y/n)	Date of Entry (Date of Submission of Complete Information for Release)	Date of Release	Date Input in ACE

3. The broker will add the following post-release data elements to the cargo release report (above) once all transactions have been filed in ACE if downtime and enforcement discretion were approved. The broker will send the completed final report to cyberincident@cbp.dhs.gov as well as the impacted Port Directors and Center Directors or their designees, along with a certified statement that all affected transactions are included in the report and have been transmitted to ACE within five business days after the expiration of CBP enforcement discretion.

Post Release						
Entry Type	Center	Date Entry Summary Filed	Date Duties, Taxes, Fees Paid	Value	Date Interest Paid	Cash Receipt Number for Interest

Any questions regarding broker cybersecurity incidents may be directed to cyberincident@cbp.dhs.gov.