CYBER INCIDENT
GUIDANCE FOR CUSTOMS BROKERS

Background: *This document provides guidance and best practices to enhance preparedness for a cyber incident on a licensed customs broker data system.*

Issued*: April 2023*

PREVENT & PROTECT: CYBERSECURITY PLANNING AND RISK MANAGEMENT

- ✓ **Maintain written cybersecurity policies and/or procedures to protect IT systems:** Follow protocols based on recognized industry frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and review policies frequently.
- ✓ **Utilize, update, and validate efficacy of IT controls:** Utilize current firewall, anti-virus, and anti-spyware software and run frequent updates; Regularly test the security of IT infrastructure through vulnerability scans; Exercise due diligence to ensure IT service providers have security measures in place.
- ✓ **Maintain up-to-date Interconnection Security Agreements (ISA):** If directly transmitting data to ACE, submit an up-to-date ISA—at least every three years—to equip CBP with accurate information on company systems and broker contacts, allowing for streamlined coordination during a cyber incident.
- ✓ **Protect your data:**
  - Frequently back up data and store all sensitive and confidential data in an encrypted format.
  - Keep backup devices physically offsite (or in the cloud) and connect backup devices to a different network.
  - Maintain originals of records, including records stored in electronic formats, within the customs territory of the U.S. in accordance with 19 CFR 111.
- ✓ **Develop plan for communicating with stakeholders about cybersecurity incidents that identifies:**
  - ***WHO*** to notify with current contact information for CBP and Partner Government Agency (PGA) contacts
  - ***WHEN*** to reach out to importer clients, system vendors, CBP, and PGA contacts
  - ***WHAT*** kind of information to share at each stage of a cyber incident
- ✓ **Manage risk:**
  - Account for supply chain risks—threats to national security, trade compliance, and PGA requirements—in business continuity plans, and identify how to manage these risks absent system access.
  - Have a risk-based process for screening new business partners and for monitoring current partners (**TIP:** Refer to the CTPAT Five Step Risk Assessment Process for basic tools, resources, and examples to consider when conducting a supply chain risk assessment.)
- ✓ **Have a plan to verify client's PGA requirements absent system access:** ACE reports and similar reporting from PGAs may help.

COMMUNICATE: INITIAL NOTIFICATION AND ONGOING STAKEHOLDER COORDINATION

1) **Immediately notify** CBP's Office of Information Technology Security Operations Center (SOC).
2) **Communicate** with CBP client representatives and relevant PGAs.
3) **Reach out to importer clients** and coordinate with CBP HQ to align messaging.
4) **Hold frequent calls** with CBP HQ and PGA contacts to provide ongoing status updates.

Note: Brokers must report any breach of records relating to Customs business no later than 72 hours as required under 19 CFR 111.21(b).

TIP: Be prepared to provide the SOC with details on the time of incident, involved parties, cause, impact, whether any Personally Identifiable Information was exposed, and any known indicators of compromise.

CBP Security Operations Center

703-921-6507

cbpsoc@cbp.dhs.gov

RESPOND: MAINTAIN MOVEMENT OF LAWFUL CARGO WHILE MANAGING RISK

- ✓ CBP may be able to work with brokers to implement downtime procedures, providing flexibility to maintain the facilitation of lawful trade and release of cargo while systems are down.

1. **Contact CBP OFO** at headquarters level to request assistance and ensure broker's downtime procedures are compliant with CBP requirements.
2. **Provide downtime letter** documenting each entry with entry numbers and other required data.
3. **Be prepared** to provide copies of appropriate documents for manual review.

- ✓ Where appropriate and legally permissible, CBP will also work with the broker to make accommodations for post-release procedures.

Other Downtime Tips and Best Practices:

- Have an offline continuity plan, including a reserve of entry numbers to use.
- Plan to fulfill PGA requirements; hard copy PGA forms alongside the commercial invoice and documentation on product specifics may assist.
- Maintain frequent communication with government stakeholders until the cyber incident has been remediated and business has resumed.
- Remember that clearance of merchandise can be provisional in nature. Requests for redelivery are possible.

RECOVER: RECONNECT SYSTEM AND WORK TO RESUME BUSINESS

- ✓ **System safety validation:** Brokers must provide evidence of system remediation before CBP will authorize reconnection to ACE.
- ✓ **Retroactive data entry:** Brokers are required to keep a full accounting of entries during cyber incidents and input that data into ACE for CBP processing.

CBP Publication No. 3163-0423.