

U.S. Department of Homeland Security

Frequently Asked Questions (FAQ)

What is Importer Security Filing (formerly known as 10+2)?

U.S. Customs and Border Protection (CBP) will be requiring an Importer Security Filing (ISF) prior to vessel loading at foreign ports. The ISF generally will consist of 10 additional data elements from U.S. importers. In addition 2 data set items will be required from carriers. The Importer Security Filing and additional data from carriers will enhance CBP's ability to identify high-risk cargo shipments.

Update from CBP – Effective December 5, 2008

Customs decided they will accept the DUNS Numbers in lieu of a complete name and address for the parties listed below. A DUNS number is unique 9 digit identification number assigned by Dun & Bradstreet (D&B)

- Manufacturer/Supplier
- Selling Party
- Buying Party
- Ship to Party
- Container Stuffing Location
- Consolidator

CBP is recommending for all importers to begin gathering the Duns numbers from their business partners. For those who do not have a Duns Number, they should be encouraged to apply for one through Dun & Bradstreet. This number will greatly decrease the amount of data entry required for filing ISF.

Will CBP implement the Importer Security Filing immediately?

The interim final rule will be published in the Federal Register on Tuesday, November 25 and will take effect 60 days after publication.

The interim final rule also includes a delayed compliance date of 12 months after the interim final rule takes effect. During this 12-month period, CBP will show restraint in enforcing the rule. CBP will take into account difficulties that importers may face in complying with the rule as long as importers are making a good faith effort and satisfactory progress toward compliance.

In addition, CBP will conduct a review, to determine any specific compliance difficulties that importers and shippers may experience in submitting all 10 data elements 24 hours before lading. The structured review will cover a range of enterprises, from small to large, and will include both integrated and nonintegrated supply chains.

Based on the information obtained during the structured review and public comment periods, CBP will conduct an analysis of the elements subject to flexibility. The analysis will examine compliance costs for various industry segments, the impact of the flexibilities, the barriers to submitting the data 24 hours prior to lading, and the benefits of collecting the data. Based upon the analysis, DHS will determine whether to eliminate, modify or maintain these requirements.

Why is CBP requiring this information?

The regulations are specifically intended to fulfill the requirements of section 203 of the Security and Accountability for Every (SAFE) Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002. The SAFE Port Act requires the Secretary of Homeland Security, acting through the Commissioner of CBP, to promulgate regulations to require the electronic transmission of additional data elements for improved high-risk targeting, including appropriate security elements of entry data for cargo destined to the United States by vessel prior to loading at foreign seaports.

How do we handle situations where despite due diligence, all of the necessary data elements are simply not available?

If an ISF importer does not know an element that is required, that party must take steps necessary to obtain the information. In some cases, business practices may have to be altered to obtain the required information in a timely fashion. CBP is committed to working with the trade to assist them in achieving full compliance and will provide guidance in the form of FAQs, posting on the CBP web site, and other outreach to the trade. For certain data elements (manufacturer (or supplier), ship to party, country of origin, and commodity Harmonized Tariff Schedule of the United States (HTSUS) number), ISF Importers will be permitted to submit an initial response or responses based on the best available data which they will have to update as soon as more precise or more accurate information is available, but in no event less than 24 hours prior to arrival at a U.S. port (or upon lading at a foreign port that is less than a 24 hour voyage to the closest U.S. port).

What about general confidentiality issues?

Importer Security Filing data is treated as law enforcement sensitive when received by CBP because it is used for national security targeting purposes. It may also be considered confidential commercial information (subject to the Trade Secrets Act), when providing the same or similar information as required on the CBP 3461 Entry Form. Therefore, CBP would assert the applicable exemptions to withhold this information from public disclosure under the Freedom of Information Act (FOIA), unless authorized by law or required by a court order.

What information is in the vessel stow plan required of carriers?

The vessel stow plan includes, for each vessel: vessel name, including international maritime organization (IMO) number; vessel operator; and voyage number. For each container: container operator, equipment number, equipment size and type, stow position, Hazmat code (if applicable,) port of lading, and port of discharge.

What will vessel stow plans be used for?

Vessel stow plan information will be used primarily to identify un-manifested containers prior to arrival into the United States. Vessel stow plans will also be used to identify the specific physical location of dangerous goods and other high-risk containerized cargo aboard vessels.

What will container status messages that are now required of carriers be used for?

Container status messages will primarily be used to track the physical movement of cargo containers as they move through the supply chain.

Who can file the Importer Security Filing?

The ISF importer or his agent will be responsible for filing the complete, accurate, and timely importer Security Filing. For the purposes of the interim final rule, ISF importer means the party causing goods to arrive within the limits of a port in the United States. For foreign cargo remaining on board, the ISF Importer is construed as the carrier. For immediate exportation (IE) and transportation and exportation (T&E) in-bond shipments, and goods to be delivered to a foreign trade zone (FTZ), the ISF importer is construed as the party filing the IE, T&E, or FTZ documentation with CBP.

What is the CBP-approved electronic data interchange system?

The current approved electronic data interchange systems for vessel stow plans are vessel Automated Manifest System (AMS), secure file transfer protocol (sFTP), and email. The current approved electronic interchange system for container status messages is sFTP. The current approved electronic data interchange systems for Importer Security Filings are vessel AMS and the Automated Broker Interface (ABI). CBP will publish a notice in the Federal Register if a different or additional electronic data interchange systems are approved.

Will the Importer Security Filing be required in all transportation modes?

This interim final rule is focused on ocean cargo. CBP is not exploring the expansion of the Importer Security Filing to other modes of transportation.

What measures will be taken as part of the Secure Freight Initiative to ensure data security, and address privacy concerns regarding the use of commercial data for counterterrorism risk-screening purposes?

To ensure data security, CBP uses standard file formatting; data transfer protocols and secure submission interfaces within its Automated Commercial System (ACS) and Automated Targeting System (ATS).

CBP considers this commercial data as business sensitive information, which may constitute trade secrets, and would protect such data from disclosure to the extent authorized by law (the Trade Secrets Act prohibits the unauthorized disclosure of confidential commercial information). As to any personally identifiable information, such information is held securely with restricted access on a need to know basis and subject to the same handling procedures as other personally identifiable data CBP routinely collects from travelers in connection with its border enforcement mission and in accordance with the Privacy Act.

As CBP endeavors to further bolster its targeting capabilities by creating new programs under the Secure Freight Initiative, it will continue to ensure that the same rigorous security and privacy protocols that exist today are scrupulously followed.

How was the Importer Security Filing requirement developed? Was the trade community/private sector involved in the development process?

CBP's close partnership with the trade community is the key reason why the interim final rule was developed in a smooth and timely fashion. The trade's input during the consultative process as well as its participation in the Advance Trade Data Initiative has been instrumental in the successful crafting of the proposal. Additionally, the Department's Advisory Committee on Commercial Operations, also known as COAC, is comprised of government and industry representatives. In early 2007, COAC made almost 40 recommendations to CBP on how to implement the security filing rule. CBP carefully studied and considered the COAC recommendations and agreed in full and/or in part to a majority of the recommendations.

What outreach activities are planned for this rule?

CBP will conduct an extended round of structured outreach activities to engage with the trade on all aspects of the rule with a series of regional seminars and trade round table discussions at all of CBP's major seaports of entry and other ports as needed or requested by the trade.

In addition, CBP will identify trade community operators who have established processes or who have successfully re-engineered processes to deliver the data timely to CBP to provide their colleagues in the community with business advice on how to comply with the regulatory requirements.

CBP will conduct seminars that focus on all topics related to this rule, including technical, operational, and process components, such as documentation adjustments (e.g., modifying the terms of letters of credit to require receipt of data to effect final payment) and developing automated solutions to track supply chain partners and commodity orders (e.g. creating vendor/supplier databases).

Will CBP accept the MID or adopt the use of standardized commercially-recognized entity identification numbers for ALL name/address elements?

CBP will not accept the MID in lieu of providing the name/address of the manufacturer or supplier of the goods on the Importer Security Filing. However, commercially accepted identification numbers may be provided in lieu of the name and address for several elements. In addition, CBP will continue to explore the potential use of the Automated Commercial Environment (ACE) ID and Participating Government Agency identifiers in the future and as ACE is developed.