

US IMPORTER SECURITY FILING: ADVANCE ELECTRONIC DATA UNDER THE SAFE FRAMEWORK MEETS THE REAL WORLD

Bryce C Blegen

Abstract

The World Customs Organization (WCO) SAFE Framework of Standards (SAFE Framework) incorporated as a core element the idea of utilisation of advance electronic information as a means for Customs to perform a security-based risk assessment of inbound consignments prior to their physical arrival in a country, allowing for detention of harmful shipments prior to their departure at origin, and more effective targeting of high-risk consignments prior to their arrival at the port of destination. The United States Importer Security Filing constitutes the first implementation of this principle into widespread practice. This article provides a comprehensive overview of the new requirements, an analysis of their impact on traders, and draws attention to certain aspects of the US initiative which may, if not modified, impede its successful implementation, and which should be considered by other countries looking to put in place similar requirements.

1. Introduction

Under the World Customs Organization (WCO) SAFE Framework of Standards (SAFE Framework), adopted at the WCO Council in June 2006, the first of the four Core Elements for customs administrations provides for the use of advance electronic information on in-bound cargo as an essential tool for Customs to perform a risk assessment on a consignment intended for import (or transit), whether the data is obtained prior to import, prior to their physical arrival, prior to their departure from origin, or even prior to their lading on an out-bound means of international transport. Regardless of timing of the advance data transmission, the idea is to give Customs more data, in an electronic form which is subject to automated analysis, at an earlier point in order to allow effective risk analysis to be performed prior to presenting the consignment for customs inspection. The intent is to enhance targeting effectiveness, allowing low-risk cargo to proceed without inspection and consignments deemed to be high risk to be inspected or interdicted. This should allow Customs to more effectively exercise its role in protecting the public from the risk of terrorist abuse of the international trading system to transport weapons of mass destruction, or their components or precursors, from one country to another, as well as to minimise disruption of legitimate trade. Aside from this anti-terrorism focus, it is evident that advance data should also allow Customs to better target smuggling or non-compliant import consignments, and is a widely accepted rationale for the implementation of new regulatory requirements in these areas.

Although the European Union (EU), Japan, and other countries are in the process of formulating advance data-related regulatory requirements, with implementation dates in some cases already set, the United

States (US) which since 9/11 has been at the forefront of formulating and enacting supply chain security initiatives, is almost certain to be the first country to roll out an advance data initiative focused on imports. On 25 November 2008, the US Department of Homeland Security, through its subdivision US Customs and Border Protection (CBP), issued an interim final rule entitled ‘Importer Security Filing and Additional Carrier Requirements’. This rather innocuously titled 57-page regulation contains what is likely to represent the single most significant change in the US import process in at least 15 years, and is the culmination of approximately two years of concentrated effort by CBP in the face of widespread trade opposition within the US. The initiative embodied in the interim final rule has become widely known as ‘10 + 2’, due to the number of key data elements required, although it is now officially known as the Importer Security Filing (ISF). It has its legal basis in Section 203 of the *Security and Accountability for Every Port Act* of 2006 (Pub. L. 109–347, 120 Stat. 1884), widely known as the ‘SAFE Port Act’, which requires the Secretary of Homeland Security to promulgate regulations to ‘require the electronic transmission to the Department [of Homeland Security] of additional data elements for improved high-risk targeting, including appropriate security elements of entry data...to be provided as advanced [*sic*] information with respect to cargo destined for importation into the United States prior to loading of such cargo on vessels at foreign seaports’. CBP’s official rationale for the ISF regulation, as included in the 25 November 2008 rule notice, was ‘the information required is that which is reasonably necessary to enable high-risk shipments to be identified so as to prevent smuggling and ensure cargo safety and security pursuant to the laws enforced and administered by CBP’. CBP announced that implementation of the ISF requirements were to go into effect, in large part, on 26 January 2009, with full implementation (and enforcement of violations) scheduled for one year later, in early 2010.

The implementation of the ISF requirements in the US is sure to have far reaching effects, as it will directly or indirectly affect all parties engaged in the sales and subsequent supply chain process related to all overseas consignments travelling by ocean vessel and entering US ports (even temporarily), even though its legal purview is limited to US-bound carriers, freight forwarders acting as ‘virtual’ carriers (the Non-Vessel Operating Common Carriers [NVOCCs]) and importers (even temporary importers) of the inbound consignments. As the first real-world example of the SAFE Framework’s advance data core element to be implemented, the US ISF regulations are worth careful examination, as they will by definition provide a precedent for other countries looking to implement similar initiatives, and already may be useful to provide insight into some of the factors that should be considered both prior to and during implementation of such initiatives. There is no doubt that the next year of phased enforcement of the ISF requirements will lead to many further lessons learned, and continued close scrutiny by international policymakers of the US ISF roll-out is warranted.

2. US import process today

In order to appreciate the significance of the changes introduced under the ISF regulations, it is important to understand the current US import process. For a number of years, ocean carriers have been required to submit advance manifest data, generally in electronic form, for goods coming into the US. Manifest data is submitted to the US Government’s Automated Manifest System (AMS), where it is used to target shipments for inspection by CBP. After the events of 9/11, advance manifest requirements were strengthened under the so-called ‘24-Hour-Rule’, promulgated under the Trade Act of 2002, which mandated both an expanded data set (see column 1 of Figure 1 below for a listing) and the requirement that manifest information be submitted ‘no later than 24 hours before the cargo is laden aboard a vessel at a foreign port’ (although in practice the data is normally required to be ready for submission at the vessel’s arrival at the port for loading, and especially in the case of consolidated cargo, even earlier). The key identifier for manifest information for shipments inbound into the US is the Bill of Lading number, which is an alphanumeric consignment reference satisfying strict requirements set out in the US Customs Regulations (19 CFR §4.7a). Carriers, freight forwarders and consolidators accepting goods via ocean

freight destined for the US issue Bill of Lading numbers for each individual consignment accepted under a schema designed to enable them to function as a unique reference for reporting to CBP. These service providers generally have direct access to the AMS, which has historically been the primary conduit for communication with CBP for port- and vessel-related activity occurring outside of the US.

Figure 1: Current Status Versus New Requirements

Current Status Versus New Requirements

<h3 style="margin: 0;">Required Manifest Data</h3> <p style="margin: 0; background-color: #e0e0e0; padding: 2px;">Generally, 24 Hrs Prior to Lading</p> <ul style="list-style-type: none"> • Bill of Lading Number • Foreign Port before vessel departs for U.S. • Carrier SCAC • Carrier Assigned Voyage Number • Date of Arrival at First U.S. Port • U.S. Port of Unlading • Quantity • Unit of measure of Quantity • First Foreign Place of Receipt • Commodity Description (or HTS-6) • Commodity Weight • Shipper Name • Shipper Address • Consignee Name • Consignee Address • Vessel Name • Vessel Country • Vessel Number • Foreign Port of Lading • Hazmat Code • Container numbers • Seal Numbers • Date of departure from Foreign Port • Time of Departure from Foreign Port 	<h3 style="margin: 0;">Security Filing Data</h3> <p style="margin: 0; background-color: #e0e0e0; padding: 2px;">ISF-10 "Regular" Cargo (3461, IT, FTZ)</p> <ul style="list-style-type: none"> • 24 Hours Prior to Lading <ul style="list-style-type: none"> • Seller (Owner) name/address • Buyer (Owner) name/address • Importer of record number • Consignee number • 24 Hours Prior to Lading--Range of Responses <ul style="list-style-type: none"> • Manufacturer (Supplier) name/address • Ship to Party • Country of Origin • Commodity HTS-6 • No Later than 24 Hours Prior to Arrival <ul style="list-style-type: none"> • Container Stuffing location • Consolidator name/address <p style="margin: 0; background-color: #e0e0e0; padding: 2px;">ISF-5 "Transit" Cargo (FROB, IE, TE)</p> <ul style="list-style-type: none"> • Booking Party Name/Address • Ship to name/address • Commodity HTS-6 • Foreign Port of Unlading • Place of Delivery <p style="margin: 0; background-color: #e0e0e0; padding: 2px;">Stow Plan Data Container Status Message (CSM) Data</p>	<h3 style="margin: 0;">Entry Data Elements</h3> <p style="margin: 0; background-color: #e0e0e0; padding: 2px;">Generally, up to 15 Days After Arrival</p> <ul style="list-style-type: none"> • Entry Number & Type • Entry – Dist & Entry – Port • Filer Code • Importer of Record • Ultimate Consignee • Surety Number • Filing Date & Time • Importing Carrier • Vessel Name • Country of Origin • Exporting Country • Exporting Date • Foreign Port of Arrival • Estimated Arrival Date • Entry Value • HSUSA (10) • Manufacturer ID <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center; margin: 0;">Identification of:</p> <ul style="list-style-type: none"> • Supply Chain Entities • Cargo Descriptions • Cargo Origins • Container Routing • Conveyance Routing </div> <p style="text-align: right; margin-top: 5px;">5/3/2009</p>
--	--	---

U.S. Customs and
Border Protection

Source: U.S. Department of Homeland Security, U.S. Customs and Border Protection 2009, 'Importer Security Filing and Additional Carrier Requirements, 10+2 Program: Importer Presentation, 02/13/2009', slide 74, http://www.cbp.gov/xp/cgov/trade/cargo_security/carriers/security_filing/

Commercial goods imported into the US are generally subject to a two-step filing process, with qualified importers entitled to file an Entry for Immediate Delivery (often referred to as a '3461' from its CBP form designation) prior to arrival of the vessel at the port, and to receive a provisional release of the goods, subject to the requirement to file a subsequent full declaration (called the Entry Summary, or '7501') within 10 working days thereafter. For both declaration types (note that there are others for special categories of merchandise, but the same time periods generally apply), the filings are done either directly (by an importer via self-filing) or via the importer's agent (the US Customs Broker) electronically to the US Government via a messaging interface called ABI (Automated Broker Interface, currently undergoing transition to a new system environment called the Automated Commercial Environment or 'ACE'). Electronic communications with ABI are conducted in a prescribed messaging format, and must be generated by a CBP-approved software application, after strict qualification testing. Filings must be done by approved filers (whether importers acting as self-filers or customs brokers filing on behalf of importer clients), each of which is identified by a unique Filer Code issued by CBP after an approval process. The Bill of Lading number of the single or multiple consignments covered by the import entry

is a required element in all importer declarations, and is utilised by CBP as the key matching element between the data submitted to the AMS system and that submitted to the ABI system

It should be noted that the data required in the advance AMS filing (see Figure 1), even as modified by the 24-hour rule, is focused on transport- and high-level commodity information, not on details of the commercial transaction underlying the consignments covered, such as buyers, sellers, other parties and service providers involved and details of origin, place of manufacture, and ultimate destination. The data provided in the import declarations does cover much of this information but is generally provided after the arrival of the consignment in the US, often several days thereafter. Since knowledge of the parties to an import transaction is a key element in determining the terrorism risk status of a consignment, the import declaration timing requirements have, as a practical matter, historically precluded CBP from effectively targeting high-risk consignments prior to lading or arrival in the US. Lack of advance data on parties to and origin of a consignment have also limited CBP's ability to tie targeting activities to party risk status (for example, a party's compliance record or membership in the Customs-Trade Partnership Against Terrorism [C-TPAT] program) until after the goods physically arrive in the port. CBP's primary purpose in promulgating the ISF regulation was to fill this perceived gap.

3. Advance data under the SAFE Framework and under ISF

The WCO SAFE Framework emphasises, with regard to Pillar 1 (Customs-to-Customs cooperation), that:

The central tenet of this pillar is the use of advance electronic information to identify high-risk containers or cargo. Using automated targeting tools, Customs administrations identify shipments that are high-risk as early as possible in the supply chain, at or before the port of departure.

Provision should be made for the automated exchange of information. Systems should therefore be based on harmonized messages and be interoperable (2007, p. 7).

While it could be argued that the above applies only to harmonised messaging between customs administrations, the SAFE Framework goes on to state in Standard 6 for customs administrations that 'The Customs administration should require advance electronic information on cargo' (2007, p. 20), and then goes into great detail in terms of what data (in terms of data elements and their definitions, which are included in the SAFE Framework after Section 1.3) may be obtained. With regard to import, it states the following:

1.3.3. Import Goods declaration: The importer or his/her agent has to submit an advance electronic import Goods declaration to the Customs at import prior to arrival of the means of transport at the first Customs office. For security purposes, Customs should not require more than the details listed in 1.3.1 (2007, p. 15).

The ISF regulations, by and large, do not refer to existing international standards, but rather explicitly enumerate and define the data elements to be provided, as well as the acceptable transmission methods. Messaging requirements for the primary interface to be used by ISF Importers, the ABI system, were published on 3 December 2008. It is notable that neither a number of the data elements themselves, nor their definitions, are in conformity with the standards set out in the WCO SAFE Framework. Nor are they in conformity with the WCO Data Model, nor, in most cases with the UN data standards. Although the US has been actively engaged in proposing modifications to the WCO SAFE Framework data standards to encompass the ISF requirements, it elected to go forward with the ISF requirements without achieving these changes. With the exception of the use of international standards-based messaging on a portion of the carrier ISF filings made in the AMS system, it appears that ISF messaging is to be based primarily on ABI-specific requirements and protocols.

4. What does the ISF rule require?

The new regulation imposes requirements on (1) ocean carriers bringing goods into the US and (2) importers, as defined in the regulation, to transmit an Importer Security Filing to CBP.

A. Carrier requirements (the ‘2’)

From ocean carriers, including the ‘virtual’ carriers known as NVOCCs being generally operating units of international freight forwarders, the regulation requires two data elements different from those already submitted as part of their AMS requirements (see Figure 1), namely the (1) stow plan and (2) container status messages. Under the new regulations, CBP must receive ‘the stow plan no later than 48 hours after the carrier’s departure from the last foreign port. For voyages less than 48 hours in duration, CBP must receive the stow plan prior to the vessel’s arrival at the first port in the United States’. Vessels exclusively carrying bulk and break bulk cargo are exempt from the ISF requirements, and do not need to submit either stow plans or status messages.

‘The vessel stow plan must include standard information relating to the vessel and each container laden on the vessel’, as indicated in Figure 1. With regard to the Container Status Message requirement, the regulations require ‘carriers to submit container status messages (CSMs) to CBP daily for certain events (see Figure 1) relating to all containers laden with cargo destined to arrive within the limits of a port... [for example, including freight to remain on board (FROB) and destined for a port outside of the United States]. CSMs created under either the American National Standards Institute (ANSI) X.12 standard or the United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport (UN EDIFACT) standard are acceptable’.

‘Carriers must submit CSMs [to CBP] no later than 24 hours after the message is entered into the carrier’s equipment tracking system’, when any of the required events occurs. Events to be reported (only if the carrier otherwise tracks or enters them into its own or client systems) include:

- (1) When the booking relating to a container which is destined to arrive within the limits of a port in the United States by vessel is confirmed;
- (2) When a container destined to arrive within the limits of a port in the United States by vessel undergoes a terminal gate inspection;
- (3) When a container, which is destined to arrive within the limits of a port in the United States by vessel, arrives or departs a facility (These events take place when a container enters or exits a port, container yard, or other facility. Generally, these CSMs are referred to as “gate-in” and “gate-out” messages.);
- (4) When a container, which is destined to arrive within the limits of a port in the United States by vessel, is loaded on or unloaded from a conveyance (This includes vessel, feeder vessel, barge, rail and truck movements. Generally, these CSMs are referred to as “loaded on” and “unloaded from” messages.);
- (5) When a vessel transporting a container, which is destined to arrive within the limits of a port in the United States by vessel, departs from or arrives at a port (These events are commonly referred to as “vessel departure” and “vessel arrival” notices.);
- (6) When a container which is destined to arrive within the limits of a port in the United States by vessel undergoes an intra-terminal movement;
- (7) When a container which is destined to arrive within the limits of a port in the United States by vessel is ordered stuffed or stripped;
- (8) When a container which is destined to arrive within the limits of a port in the United States by vessel is confirmed stuffed or stripped; and

(9) When a container which is destined to arrive within the limits of a port in the United States by vessel is shipped for heavy repair.

CBP has offered carriers the option of transmitting all CSMs, rather than just those relating to containers destined for the United States or relating only to the required events. By doing so, however, the carrier authorises CBP to access and use those data for targeting.

B. Importer requirements (the ‘10’, or sometimes, the ‘5’)

Under the new ISF regulations, there are two categories of Importer Security Filing. The first applies to consignments which (a) are to remain on board the vessel while in the US port or ports (‘freight remaining on board’, or FROB), or (b) will move under transit procedures for transportation onward to a final destination in another country. The party designated by the ISF regulations as the ‘ISF Importer’, and therefore responsible for the ISF filing, is deemed to be the carrier in the case of FROB and the party filing the transit document for the transit category. This designation appears to be designed to distinguish application of the ISF regulations’ requirements from those applying to classic US concept of ‘Importer of Record’, which has its own set of obligations under US customs law and regulation. This brings the party responsible for FROB (who would not otherwise be deemed an Importer under US customs law) within the coverage of the ISF regulations.

Note that consignments in temporary transit status destined to a Foreign Trade Zone (FTZ) in the US are subject to the full 10-element ISF requirements (see below for the details of ISF-10). Consignments originally intended to transit the US for re-export but which undergo a change in status in transit (for example, re-designated for an import or a FTZ) become subject to the 10-element requirement. Otherwise, however, for the ISF-5 importer category, a 5-element advance data submission is required. Note that only two of these, elements 4 and 5, are also required under the 10-element ISF category. The elements, and their definitions, are as follows:

- (1) *Booking party*. Name and address of the party who initiates the reservation of the cargo space for the shipment. A widely recognized commercially accepted identification number for this party may be provided in lieu of the name and address (Dun and Bradstreet Data Universal Numbering System, or ‘DUNS’ numbers are listed as being acceptable).
- (2) *Foreign port of unloading*. Port code for the foreign port of unloading at the intended final destination.
- (3) *Place of delivery*. City code for the place of delivery.
- (4) *Ship to party*. Name and address of the first deliver-to party scheduled to physically receive the goods after the goods have been released from customs custody. A widely recognized commercially accepted identification number for this party may be provided in lieu of the name and address (DUNS or Facilities Information and Resources Management System ‘FIRMS’ numbers are listed as being acceptable).
- (5) *Commodity HTSUS number*. Duty/statistical reporting number under which the article is classified in the Harmonized Tariff Schedule of the United States (HTSUS). The HTSUS number must be provided to the six digit level. The HTSUS number may be provided to the 10-digit level.

The second ISF category applies to all consignments destined for import (whether upon arrival or after storage or processing in a FTZ). The ISF consists in general of 10 elements, unless an element is specifically exempted. The 10 elements are as follows: (1) Seller; (2) Buyer; (3) Importer of record number/Foreign trade zone applicant identification number; (4) Consignee number(s); (5) Manufacturer (or supplier); (6) Ship to party; (7) Country of origin; (8) Commodity HTSUS number; (9) Container stuffing location; and (10) Consolidator (stuffer). The manufacturer (or supplier), country of origin, and commodity Harmonized Tariff Schedule of the United States (HTSUS) number must be linked to one another at the consignment line item level, meaning that each combination of commodity, origin, and manufacturer/supplier in a consignment would need to be reported as a separate line in the ISF.

The definitions of the ISF-10 data elements are as follows:

(1) *Seller*. Name and address of the last known entity by whom the goods are sold or agreed to be sold. If the goods are to be imported otherwise than in pursuance of a purchase, the name and address of the owner of the goods must be provided. A widely recognised commercially accepted identification number for this party may be provided in lieu of the name and address (DUNS numbers are listed as being acceptable).

(2) *Buyer*. Name and address of the last known entity to whom the goods are sold or agreed to be sold. If the goods are to be imported otherwise than in pursuance of a purchase, the name and address of the owner of the goods must be provided. A widely recognized commercially accepted identification number for this party may be provided in lieu of the name and address (DUNS numbers are listed as being acceptable).

(3) *Importer of record number/Foreign trade zone applicant identification number*. Internal Revenue Service (IRS) number, Employer Identification Number (EIN), Social Security Number (SSN), or CBP assigned number of the entity liable for payment of all duties and responsible for meeting all statutory and regulatory requirements incurred as a result of importation. For goods intended to be delivered to a foreign trade zone (FTZ), the IRS number, EIN, SSN, or CBP assigned number of the party filing the FTZ documentation with CBP must be provided.

(4) *Consignee number(s)*. Internal Revenue Service (IRS) number, Employer Identification Number (EIN), Social Security Number (SSN), or CBP assigned number of the individual(s) or firm(s) in the United States on whose account the merchandise is shipped.

(5) *Manufacturer (or supplier)*. Name and address of the entity that last manufactures, assembles, produces, or grows the commodity or name and address of the party supplying the finished goods in the country from which the goods are leaving. In the alternative the name and address of the manufacturer (or supplier) that is currently required by the import laws, rules and regulations of the United States (i.e., entry procedures) may be provided (this is the information that is used to create the existing manufacturer identification (MID) number for entry purposes). A widely recognized commercially accepted identification number for this party may be provided in lieu of the name and address (DUNS numbers are listed as being acceptable).

(6) *Ship to party*. Name and address of the first deliver-to party scheduled to physically receive the goods after the goods have been released from customs custody. A widely recognized commercially accepted identification number for this party may be provided in lieu of the name and address (DUNS or FIRMS numbers are listed as being acceptable).

(7) *Country of origin*. Country of manufacture, production, or growth of the article, based upon the import laws, rules and regulations of the United States.

(8) *Commodity HTSUS number*. Duty/statistical reporting number under which the article is classified in the Harmonized Tariff Schedule of the United States (HTSUS). The HTSUS number must be provided to the six digit level. The HTSUS number may be provided up to the 10-digit level. This element can only be used for entry purposes if it is provided at the 10-digit level or greater by the importer of record or its licensed customs broker.

(9) *Container stuffing location*. Name and address(es) of the physical location(s) where the goods were stuffed into the container. For break bulk shipments, as defined in § 149.1 of this part, the name and address(es) of the physical location(s) where the goods were made “ship ready” must be provided. A widely recognized commercially accepted identification number for this element may be provided in lieu of the name and address (DUNS numbers are listed as being acceptable).

(10) *Consolidator (stuffer)*. Name and address of the party who stuffed the container or arranged for the stuffing of the container. For break bulk shipments, as defined in § 149.1 of this part, the name and address of the party who made the goods “ship ready” or the party who arranged for the goods to be made “ship ready” must be provided. A widely recognized commercially accepted identification

number for this party may be provided in lieu of the name and address (DUNS numbers are listed as being acceptable).

In terms of timing, submission of the ISF to CBP, via one of the two authorised electronic systems (ABI or AMS), must be done no later than 24 hours before the cargo is laden aboard a vessel destined to the US. An exception exists for FROB, for which the Importer Security Filing is required any time prior to lading. For the initial year, and as part of the ‘interim’ portion of the ISF rule, CBP is being ‘flexible’ for Importer Security Filing elements 5 through 8, being Manufacturer/ supplier, Ship-to party, Country of origin, Commodity HTSUS number, in that while data must be provided for all four elements by the time of the pre-lading filing deadline, the data within these elements can be general or summary data which is then refined and amended up to a time ‘no later than 24 hours prior to arrival in a US port (or upon lading at the foreign port if that is later than 24 hours prior to arrival)’. Further flexibility is being provided on elements 9 and 10 (Container stuffing location; and Consolidator/stuffer), in that they will not required to be submitted until the same 24-hour prior to arrival deadline as the final data for elements 5-8.

For all ISF filings, CBP will transmit an electronic acknowledgement to the filer of an ISF, and will include a unique identification number. That unique number can be used by the Importer Security Filing filer to amend an Importer Security Filing, as in the case when it adds data or changes data as more precise information becomes available. It should be noted, however, that as of early 2009, a number of uncertainties continued to exist in the details of ISF message transmittal, its timing, and how the various parties which need to be aware of the transmittal and acceptance (or complete or partial rejection) on a particular consignment represented by a bill of lading number will have access to that information.

It should also be noted that the ISF regulations provide the opportunity for importers to file their complete customs declaration at the time of ISF filing, which eliminates the need for subsequent filing of the customs entry after arrival at the US port. Importers who wish to take advantage of this (potential cost saving) opportunity must make the filing in the ABI system, either as an authorised direct filer or via a US customs broker, and must use the full HTSUS number in the ISF, not the abbreviated 6-digit number. Due to the timing issues and some of the hurdles discussed below, it is unlikely that many importers will take advantage of this option, at least initially.

5. Enforcement and phase-in

As noted, the ISF regulations went into effect on Monday 26 January 2009. Failure to comply with the requirement of timely submission of a complete ISF subjects the party obligated under the regulation (the ISF Importer) to pay US\$5,000 in liquidated damages per incident, which is defined at the ISF consignment level. For a single vessel (which may incorporate a very large number of ISF consignments), the liquidated damages are capped at US\$100,000. Because the ISF institutes a new customs bonding requirement to cover the ISF obligation, and mandates that for each ISF, either the ISF Importer or its agent and the carrier be covered by a bond, CBP will be able to issue a bill for liquidated damages directly to the bond carrier (this is the same mechanism currently used for late filing of import declarations).

CBP has indicated that it recognises that the ISF regulations represent a major change for the trade community, and have stated that ‘in order to provide the trade sufficient time to adjust to the new requirements and in consideration of the business process changes that may be necessary to achieve full compliance, CBP will show restraint in enforcing the rule, taking into account difficulties that importers may face in complying with the rule, so long as importers are making satisfactory progress toward compliance and are making a good faith effort to comply with the rule to the extent of their current ability. This policy will last for twelve months after the effective date and will apply to all aspects of the filing rule’. CBP has also indicated that it does not intend to use the ISF regulations as a basis to issue ‘Do Not Load’ orders, although it reserves the right to do so if a national security threat is perceived.

6. ISF impact on carrier and forwarder industry

For carriers and freight forwarders operating as NVOCCs, and already serving the US market, the ISF and its requirements relating to the '2' are basically an enhancement of the already existing 24-hour rule manifest process, and should not, in and of themselves, represent an overwhelming challenge in terms of new process. The requirements for the ISF-5 applicable to FROB, do, however, represent a significant new compliance burden on carriers, but only if they route cargo to include FROB while visiting US ports. Perhaps the most significant challenge for the carrier/freight forwarder community will be the necessity to allocate bill of lading numbers conforming to the CBP requirements to their overseas service provider and consigner network sufficiently in advance to allow ISF Importer filing, to devise methods to effectively track both their own and importer ISF filings, link them to individual containers for their own filings, communicate status to all affected parties, and to ensure that delays related to ISF submission by the importers or their agents do not unduly delay loading, clogging the ports.

Although the ISF regulation explicitly states that carriers and freight forwarders operating as NVOCCs are responsible under the regulation ONLY for their '2' filings, and not for the ISF Importer obligations, as a practical matter many consignments move under door-to-door or similar arrangements under which the service provider is responsible not only to ensure the movement of the shipment, but also to provide export filing services in the port of departure and import clearance in the port of arrival. It seems likely that in many cases, providers will be asked by their customers to add the ISF filing to their menu of services. Since successful filing requires the gathering of a large amount of data at the port of departure, this will lead to a slower process, as providers gather the required information from their customers and the customers' suppliers. Especially in multi-party consolidation situations, service providers (possibly multiple per container) will not wish to undergo the risk of being responsible for all or part of a container on which all required ISFs have not been filed, which may lead to new and time-consuming verification processes prior to loading. A further complicating factor is that significant differences in functionality and data availability exist in the ISF protocols in the AMS system versus the ABI system, which may limit the feasibility of doing (in particular) ISF-10 filings in the AMS system.

7. ISF impact on US importers and overseas suppliers

Notwithstanding the above, it seems fair to say that the major burden of the ISF will fall on the traditional US import community and its overseas supply base, in particular those that transport most goods via sea, and which typically import smaller consignments packed in consolidated containers. The bulk of data relating to an imported consignment and the parties associated with it has historically been in the hands of the US importer of record, and, unless a self-filer, its customs broker, which had up to two weeks after arrival of a shipment in a US port to collect, validate and file the information. Moreover, in order to import into the US at all, the US importer and/or its broker had gone through the process of obtaining a Customs bond, an EIN number and a filer code, had connectivity (directly or indirectly) with ABI, and could be assumed to be familiar with the expectations of CBP in terms of data elements such as country of origin and HTSUS classification. The freight forwarder and its overseas network, in collaboration with the overseas supplier, was relied on to handle the formalities and steps necessary to get a consignment exported and on a vessel at the port of origin, and the US importer (even if an overseas non-resident importer) could rely on its personnel or agents in the US to handle US requirements.

The ISF, particularly ISF-10, has turned this situation on its head, and represents a radical departure from the status quo. It is true, as CBP states, that most of the data elements required under the ISF were required before. But they were required at a point in time typically 15-45 days later, and from different parties, and they were never all required at one time as a pre-requisite for the loading of a consignment onto a vessel. The ISF-10 requires the amalgamation and submission at one time of transport (data elements 6, 9, 10 + the bill of lading number), commercial (data elements 1 through 5), and compliance (elements 7

and 8) data prior to physical movement of the consignment. Previously, the transport data was either not reportable or else easily ascertainable from the record of the transport after it happened; the commercial data was reported by the party best able to obtain accurate information, namely the importer (generally either a party to the commercial transaction or closely linked to one or more of them), and at a point in time when the goods were physically in the US and therefore within the jurisdiction of CBP, and the compliance data was provided by either a licensed expert (a US customs broker) or the importer familiar with the laws of the US or at least able to access that expertise. Perhaps some importers, especially the larger ones, have most or even all of the data required by ISF in their ERP or other systems, through linkages with their supply chain service providers. But it is much more likely that they have only the commercial data, or perhaps the commercial and compliance data (linked to invoice and part numbers), and the service providers, usually multiple providers in multiple roles, have the transport data (or that portion thereof that relates to them), linked to a bill of lading. Since there has historically been no business need to link these disparate data universes, it is not an easy task to get the entire dataset in one place, especially at a time prior to loading.

It should also be noted that the ISF data elements are defined in light of traditional US customs law and practice. Country of origin is to be indicated in accordance with US origin rules (which vary from those in the EU and elsewhere), and commodity tariff codes (whether at the 6 or optional 10-digit level) are to be provided in accordance with US classification practice. Similarly, data elements 3 and 4 under the ISF require the provision of US official entity identification numbers which, while sometimes known at the time of import filing, are often difficult to obtain or which may be subject to confidentiality concerns, especially prior to the loading of the consignment, and if given into the hands of overseas service providers. As a practical matter, the fact that the ISF must be submitted prior to the consignment's loading at the overseas port may create a good deal of difficulty in ensuring data quality if overseas personnel are making determinations on which data to use. Processes and service providers used for the ISF should be evaluated in light of their ability to meet the US standards and have access to accurate data.

The name '10+2' was always somewhat deceptive, and has now been abandoned in favour of the ISF. Nevertheless, the core of the regulations still summarises datasets related to '2', for the carriers, '10', for most importers, and now '5', for certain categories of merchandise. It is imperative, especially for persons not familiar with current US import processes, to understand that CBP is assuming that parties subject to this regulation already know that they must also provide other data, such as bill of lading numbers, filer identification codes, customs bond codes, and date and time information relevant to the consignments covered by the ISF along with the ISF message itself. Since CBP and members of the US trade community have known that these requirements apply to virtually every electronic transaction made with US Government systems like ABI and AMS, it is assumed that all parties dealing with the ISF will also be aware of them. Because the data is being assembled much earlier in the import process than previously, and at the port of origin prior to lading, it is important that these additional requirements be considered and satisfied while putting the required ISF processes in place, especially if the transaction is subject to DDP Incoterms or the ISF importer is a non-resident importer into the US.

8. ISF filing: changed processes and cost burdens

There are two basic alternatives: the ISF importer requires its supply chain service providers to provide it (the importer) with the transport-related ISF data, and the importer (or its agent) takes on the burden of amalgamating that data with the commercial and compliance data, making the ISF filing, and returning the acknowledgement to the service provider loading the consignment at the point of origin in a timely manner. Or, the importer provides the service provider with its commercial and compliance data (unless the service provider has that responsibility) related to the consignment in time for the service provider to amalgamate the data, make the ISF filing, and get an acknowledgment prior to loading. Both scenarios may have pluses and minuses, and depend in part on the circumstances of the companies

involved. Clearly, for a service provider to take on the burden of the ISF, it will demand compensation through additional fees. It will most likely also impose strict requirements on the importer to provide its commercial information in a timely manner, or refuse to perform the ISF transmission (which may result in the goods staying at the port). The importer cannot, however, pass off its legal liability to CBP for ISF compliance, and, being subject to fines for infractions, may determine that it is better off ensuring the accuracy and timely filing of the ISF itself.

In the run up to the ISF regulations, and also in the CBP responses to trade comments made in the rulemaking process, CBP took the position that the ISF was focused on the minimisation of security risks, in particular those from potential terrorist activity. Many statements were made that indicated that ISF responsibility for strict data accuracy and even strict timing was not the focus; instead CBP states in the ISF regulation notice that ‘Where the ISF Importer is not reasonably able to verify the information, the regulations allow the party to submit the information on the basis of what it reasonably believes... this rule provides flexibilities with respect to certain elements of Importer Security Filings such as the ability to provide a range of possible responses based on the best data available in lieu of a single specific response’.

Yet parties making ISF filings would do well to keep in mind that an importer is otherwise responsible under US customs law and regulations for the accuracy of the data contained in its declarations, and the jury is quite literally still out on how this standard will ultimately be applied to the ISF. Moreover, CBP has already signalled that it will track the overall quality of ISF Importer filings, and even provide ‘report cards’. And as the first step in what is now a potentially three-step standard import filing process, it is not only possible but quite likely that CBP’s systems will perform comparisons of the data provided in the ISF versus that provided in the later import entry filings, and that discrepancies will be either deemed errors or become a factor in the compliance rating of the parties involved. Indeed, such data analysis is directly in line with the stated reasoning behind incorporation of advance electronic data as a core element of the SAFE Framework, as being an effective tool in customs risk-based targeting of high risk consignments or parties involved in the supply chain (whether that risk relates to terrorism, smuggling or non-compliance).

Aside from the costs associated with additional service fees and investments in IT, one should not overlook the likelihood of additional inventory, demurrage and storage costs related to delays in gathering the data prior to submission of the ISF. Ultimately, the increased costs will be borne by the US consumer, and CBP has itself estimated the cost impact of rule implementation to be on the order of US\$7.6 to US\$56 billion over the next ten years. This is not a trivial amount (and some commentators think the true cost will be even higher) at a time when the global economy is in a severe downturn and protectionism is on the rise.

It is certain that new ISF-related service offerings and fees are being negotiated around the world as you read this, and it may be some time before best practices develop in this area. The impact of Incoterms on the ISF, and who bears which portion of the data provision, amalgamation, transmission and cost responsibility associated therewith, will undoubtedly be the subject of much discussion between sellers, buyers, importers and CBP for years to come.

9. ISF in the global context: the future of advance electronic data initiatives

As formulated under the WCO Safe Framework, advance electronic data on consignments moving in international trade was intended to be a tool for Customs to better enable it to target high-risk consignments at a point in time earlier than the goods were presented for customs inspection. Data to be collected was to be limited to a specified set of elements, with standard definitions. Data collection

was to be done under national law by the national customs administration, and the collected data could be shared between administrations. Because advance data was contemplated as a consignment moves outbound (that is, is exported) and as it later moves inbound (is imported), explicit provision was made for transmission of the outbound data and subsequent risk analysis by the exporting country (which should, arguably, be in the best position to know the risk status of its exporters) to the importing country, where it could be used in lieu of a second trader-based inbound advance electronic message in the risk analysis prior to consignment arrival. Early pilots between the EU and its neighboring countries have proven the effectiveness of this concept, both in terms of risk-targeting and cost. Because this concept contemplates international standards-based cooperation between origin and destination administrations, it allows both a more effective risk assessment at an earlier time (perhaps early enough to catch the risk-laden goods before they are able to arrive at their point of deployment), and leverages already existing international supply chain milestones (for example, export filing, manifest filing, import filing) and parties thereto (for example, exporter, Customs in the country of departure, carrier/forwarder, Customs in the country of arrival, importer) in a way which could, at least in theory, increase effective risk targeting on international consignments without a significant incremental cost for the legitimate trader.

Yet, as outlined in more detail above, the first real-world implementation of the concept, namely the US ISF regulations, may well prove that an attractive concept in theory is a completely different animal when put into practice. It seems likely that the ISF may achieve its underlying goal of giving CBP better data much earlier to make its risk targeting more effective. Because, however, it is not in conformity with the standards set by the SAFE Framework, and utilises data elements, definitions, and messaging formats which, although in many cases rooted in longstanding US import processes and legal traditions, are neither known nor in use overseas, which is where a good deal of its impact falls, it seems likely to be burdensome in terms of cost and process-related delays. Furthermore, the concept of Customs-to-Customs exchange of risk information on consignments which was so prominently featured in the SAFE Framework is completely missing in the ISF implementation. Even though the EU is on track to implement its own inbound and outbound advance electronic data requirements later this year (although it seems the July deadline may be delayed), the disconnects between the EU outbound data set (which is quite closely linked to the SAFE Framework data set) and the US inbound ISF data set ensure that traders will have to be prepared to comply with both on an ocean-bound shipment from Rotterdam to New York, and almost certainly still do a European export filing and a US import filing as well. That is sure to lead to cost increases for the trader, and does not take advantage of the efficiency gains contemplated by the WCO SAFE Framework.

10. Conclusions

It is still much too early to ascertain what lessons the planned implementation of ISF, or subsequent advance electronic data initiatives planned by the EU and others will bring. But the success of all such initiatives is dependent on their successful adoption by the members of trade communities affected, and by effectively moving the borders outward, customs administrations which impose such requirements have to be cognisant of the fact that their initiatives affect a much broader community than the members of the trade in their own country, over whom they have legal jurisdiction. Communication of requirements to overseas traders, and achieving success in their adoption and implementation of them, is never an easy task when multiple cultures and languages are involved. In a time of global economic uncertainty, these difficulties are magnified, especially where what is expected is not international standards-based and does not leverage what is already required, familiar, and in-place in the exporting country. There is no doubt that a risk management-based approach to international trade can be a win-win situation between customs administrations looking to increase productivity and traders looking to reduce costs through efficient border crossings for their goods, nor is there any doubt that advance electronic data can increase both customs productivity through improved risk targeting, which should speed processing for

legitimate trade. But customs administrations cannot lose sight of the fact that data integrity and efficient automation are predicated on effective data-sharing, whether between trade and Customs or Customs-to-Customs, and on them playing an active role in ensuring new requirements do not simply mean new burdens for legitimate trade. As the US ISF implementation plays out over the next year, it should be carefully looked at by other customs administrations prior to their implementing similar initiatives, and by the WCO in its further work to keep the SAFE Framework up to date and to further develop the standards-based approach.

References

- U.S. Department of Homeland Security 2008a, 'Part II: Department of Homeland Security, U.S. Customs and Border Protection, 19 CFR Parts 4, 12, 18, et al. Importer Security Filing and Additional Carrier Requirements; Final Rule', Federal Register, vol. 73, no. 228, 25 November 2008, Bureau of Customs and Border Protection, Department of Homeland Security, Washington, DC.
- U.S. Department of Homeland Security, U.S. Customs and Border Protection 2008b, *Regulatory assessment and final regulatory flexibility analysis for the Interim Final Rule: Importer Security Filing and additional carrier requirements: Cost, benefit, and feasibility study as required by Section 203(c) of the SAFE Port Act, 06 November 2008*, report prepared by Industrial Economics, Incorporated, Cambridge, MA.
- U.S. Department of Homeland Security, U.S. Customs and Border Protection 2009, 'Importer Security Filing and Additional Carrier Requirements, 10+2 Program: Importer Presentation, 02/13/2009', slide 74, www.cbp.gov/xp/cgov/trade/cargo_security/carriers/security_filing/.
- World Customs Organization (WCO) 2006, *WCO SAFE Framework of Standards to secure and facilitate global trade*, WCO, Brussels.

Bryce C Blegen



Bryce Blegen is CEO of Trusted Trade Alliance LLC, responsible for managing the organisation's global activities from its headquarters in Vancouver, Washington, USA. He is also Regional Manager, Americas, for the Centre for Customs & Excise Studies, University of Canberra. As a US attorney specialising in global customs compliance and trade issues, Bryce has been active in spearheading customs simplification and trade facilitation initiatives in the US, Mexico, Europe and China, working closely with trade associations and government officials. He has been a member of the Legal and Transition/Software Committees of US Customs and Border Protection's Trade Support Network since 2004, and served as co-chair of the 2008 World Customs Forum at the World Customs Organization in Brussels. He is a frequent speaker on customs and trade topics in the US and Europe.

Bryce received a Juris Doctor and a Master of Arts in International Studies from the University of Denver in 1989 and was admitted as an attorney in Illinois in 1990.