



*Comments on the*

***“International Container Standards Organization”***

***and its Effort to Propose New Standards for***

***Container Security Technologies***

***July 26, 2006***

General Electric (GE), and several other companies (including Siemens and Mitsubishi Corporation) with a financial interest in the promotion of the GE “CommerceGuard” “container security device” (CSD) product recently announced the formation of a new organization -- the International Container Standards Organization (ICSO) – for the stated purpose of establishing “global standards” for container security devices.

While there is nothing surprising about GE trying to promote and protect its own business interests, this is an unnecessary and counterproductive initiative that is inconsistent with the extensive efforts of international ocean carriers, terminal operators and technology developers at the International Standards Organization (ISO). It is also a strange coincidence that GE would undertake this initiative just as the ISO is about to finalize its years of efforts in developing a consensus international RFID container security technology standard – a standard that differs significantly from GE’s product.

The development of international standards is usually done through the broadly accepted International Standards Organization. The ISO works hard to develop standards that are not proprietary in nature, by having competitors and users jointly develop a technology standard that is not driven by a specific product. While at times difficult and contentious, the process is deliberately designed to avoid proprietary standards that favor one manufacturer’s product, while meeting the user community’s broader needs.

The ICSO effort appears intended to deviate from the extensive work already done to date by technology developers, ocean carriers and marine terminal operators in developing a common, broadly accepted international standard for RFID container security technology at the ISO. It is essential that the maritime industry, port facilities,

shippers and others engaged in global commerce have a single uniform international container security technology standard for any device that needs to be read by fixed readers at ports and other locations around the world. It would be unreasonable to expect port facilities and shippers to install devices, reading infrastructures and data networks specifically for a GE or a new ICSO CSD product that differs from the international standard the industry has just spent the last two years developing at the ISO. In addition, it is premature to develop a standard for a “container security device” before industry and governments have discussed and agreed upon the security requirements should be for such devices.

The following are some additional observations regarding the stated goal of ICSO.

### **1. Existing ISO Standard Setting Efforts**

For the past two years, liner shipping companies, marine terminal operators and technology companies have been developing at the ISO an international standard for electronic container seals (e-seals) using RFID technology. U.S. Department of Homeland Security representatives have participated as observers in these ISO standard-setting deliberations for the past 12-14 months. That standard is on schedule to be finalized by the end of the year, subject to the outcome of another set of test projects that technology developers will be undertaking this summer in cooperation with marine terminal operators. These projects follow other tests performed earlier this year by the technology developers, liner shipping companies and marine terminal operators.

The ISO container e-seal standard sets out detailed operational requirements -- identified and agreed-upon in an extensive, cooperative process between the carriers, marine terminals operators and the technology developers. The standard-based RFID seal would work in two radio frequencies in recognition of the fact that no single frequency currently is publicly available in all trading nations around the world. GE has been fully aware of, and has at times participated in, the deliberative ISO process specifically established to identify the operational requirements for RFID container *seals*. While the operational requirements and reading infrastructure for an RFID “*container security device*” logically should be the same as for an RFID container seal (e.g. read distance, read speed, different container handling scenarios by different types of equipment in marine terminals), GE explicitly declined to participate in that part of the ISO process.

### **2. The Technology To Be Used for Container Security**

While the possible technology for security devices affixed to containers has been described as using various technologies from RFID to wireless/satellite devices, the most commonly discussed and proposed technology is, at the current time, RFID. This is also the technology assumption for the ISO container e-seal standard. This is a discussion of substantial importance, because it affects: 1) what kind of reading infrastructure would

need to be installed for the devices to be operational, and 2) what kind of functionality one could obtain from the device.

If RFID is to be used as the technology for CSDs, the container devices would require a global reading infrastructure to be built and installed at ports around the world, and presumably at inland locations as well depending on how the product is to be used. That infrastructure does not presently exist, and will have to be installed on thousands of different property owners' premises.

It is for that reason that, for the past two years, ocean carriers, marine terminal operators, and technology developers have worked at the ISO to develop a non-proprietary, open architecture RFID container technology standard. If RFID is to be used, why should ICSO be created to establish a different set of standards than what the ISO has developed over the last two years for RFID electronic container seals, with very extensive effort and input by technology providers, terminal operators and carriers? Is it because the GE product is not compatible with this ISO standard?

The ISO container RFID e-seal standard deals with radio frequencies, container handling scenarios in marine terminals, read distances, reliability measures, communication protocols, and many other features that would be shared also by a container security device (CSD). GE has followed the ISO standards development process closely, but has consciously chosen not to participate in that important part of the ISO process. It would appear that GE is establishing ICSO in order to bypass the extensive work product being developed by the ISO and to design an independent standard and process that it and its "CommerceGuard" business associates would control. And, it has done so without any explanation of why the international standard being finalized by the ISO for RFID container seals would not be appropriate for application to RFID CSDs – however such devices may be defined ultimately. It seems reasonably clear that marine terminal operators around the world would have little interest in installing at their facilities two different reading infrastructures – one for ISO standard based container e-seals and one for GE's product. Such a result would defeat the entire purpose of an agreed-upon, international standard. Yet, that seems to be the purpose of the ICSO effort.

### **3. Definition of a "Container Security Device" (CSD)**

One may argue that the GE container security device is not a container seal and therefore needs a separate technology standard. Two observations are relevant to such an argument.

*A. Definition of Requirements:* First, there is no agreement about the definition or the requirements of a "container security device". While there may be legitimate differences of opinion regarding the security value of container seals, the function and operational requirements of container seals are clearly defined and well understood in the U.S. and internationally, by both industry and governments. Thus, the development of

the electronic container seal standard in the ISO is based on a common understanding of what a seal is and what it is expected to accomplish.

The same is not true for CSDs. There is no agreed definition of a CSD or what the functional requirements for such devices should be. It would appear that the ICSO wants to establish what those functional requirements should be at the same time that it also designs the technology standards that should be used to meet its own defined requirements.

Instead, the owners, operators and users of containers would expect that governments, which have the key role in defining security requirements and protocols for containerized cargo security, should work with the industry to identify and define the security requirements *before* the developer and promoter of one type of device creates its own organization in an attempt to define what the international standard for the device should be.

Before developing a standard for a product, it is necessary to discuss and reach a clear agreement on what the product needs to do. What specific thing must a CSD do that a container seal does not do? What specific events must be captured and recorded? Should it record the opening of just one door on the container or must it be able to capture either door opening? Is capturing entry through the doors enough or must it detect entry into the container through the walls, ceiling or floor? Does the device have to detect conditions other than entry intrusion (i.e., “Advanced CSD” concept)? In this regard, GE’s “CommerceGuard” and other similar devices do not impede entry into a container, do not detect what is actually in a container, and do not “secure” a container. Instead, the current product is intended to record whether the right side door on a container has been opened.

GE has advocated before the U.S. Congress that a CSD must “positively identify the container.” It is not clear why this, for example, should be a required element of a CSD. In fact, there are arguments for why this should *not* be part of such a device, particularly as it would appear to require the device to have a “write” capability (i.e., the ability of third parties to write new information into the device), which could create security vulnerabilities for the device that have not been addressed. (See further discussion under Item 7 below.)

*B. Commonly Developed and Accepted Standards:* While the necessary definition of the requirements of a “container security device” has not yet occurred, it would seem logical that, once that task is completed, any such device using RFID technology should be designed to be compatible with the RFID container seal security technology standard that the ISO process has constructed over the last two years with input from interested stakeholders from around the world. It would make no sense for port facilities around the world to have one RFID reading infrastructure for ISO compliant electronic container seals and for GE to expect them to install a different reading infrastructure for GE devices.

Further, any RFID container technology reading infrastructure should meet the industry's operational objectives and requirements as well as providing the appropriate container security readings. Terminal operators, carriers and technology developers have been working extensively to build an acceptable ISO RFID container technology standard. There has been no explanation from GE or the ICSO why that standard cannot be used to also read RFID container security devices, however they may ultimately be defined.

#### **4. Reading System Operation and Control**

If RFID technology were to be used for container security devices, it would require a global infrastructure of readers, presumably at marine terminals, and likely at other locations.<sup>1</sup> The operating assumption within the work done to date in the ISO is that the readers for the RFID devices, the information derived from the readings of container RFID devices, and the operational responsibility for those readers would rest with the marine terminal operators. This does not appear to be the assumption of the GE "CommerceGuard" device and its associated information system.

This raises a host of unanswered, very significant questions and concerns. When RFID container devices are read, who owns and controls the data? Who is informed when readings indicate that a container door has been opened? Who is responsible for acting on that information, pursuant to what protocols with the local government? Will marine terminal operators without a financial interest in the CSD product agree to install such readers on their property, knowing that they could cause thousands of containers to be stopped and investigated for benign events, such as the fact that a customs authority has inspected the container before it arrived at the port?

Unlike other container security technologies, GE apparently wants to create, own and control the global data base of container readings done by its proprietary reader infrastructure. Their commercial and financial interest in doing so is not a security requirement. Nor has it been accepted by container owners and users. In contrast, the ISO e-seal standard explicitly requires that ISO compliant seals "shall have the ability to be interrogated by a universal, non-proprietary reading device".

Finally, if proprietary information derived from the container reading infrastructure were to become the property of the CSD vendor, then what restrictions would there be on the use and distribution of that data? This too is an issue of significant and legitimate interest to governments and to container users.

---

<sup>1</sup> As noted earlier, CSDs based on satellite technology would not face the some of the complexities resulting from the need to install, operate and maintain a global array of fixed readers, in many different countries, on may different entities' properties.

## **5. Standards for Device Reliability**

The industry does not have confirmation of the “CommerceGuard” device’s reliability. In the U.S. Congress, GE has advocated a 99% reliability standard. This is unacceptable, and would create far too many false alarms. By comparison, the ISO e-seal standard requires 99.99% reliability of compliant e-seals.

## **6. Relationship to Government Security Policy**

The ISO’s e-seal standard setting work has been undertaken with a relatively clear and commonly understood government policy framework in mind. The work has been undertaken on the assumption that the U.S. (and perhaps other governments) might establish a mandatory container seal verification regime on all loaded containers to be stowed on vessels destined for the U.S. Because manual seal verification on a global scale would be impractical, such a mandatory rule would necessitate a global electronic container seal reading infrastructure at all port facilities loading containers for the U.S. if it were to be implemented. While it was not clear whether the government would establish such a requirement because the security benefits are arguable, the operational problems would be substantial, and the costs would be high, it was clear that a universally applicable container technology and business process would be required if governments did establish such a requirement.

Government’s policy intent and framework for CSDs is not yet established. It is important that such a discussion *precede* an international standard setting. It is essential that the industry know what governments would want accomplished by a CSD. It is essential that there be an understanding and agreement on the data elements to be captured in a CSD. It is also important to understand how such devices would be read and what protocols would govern their use. For example, if CSDs are to be read at foreign load ports, who is to do the reading? For example, are CSDs to be encouraged as a voluntary measure for Tier 3 C-TPAT importers (as proposed in some pending U.S. legislation), or are they to be required for such importers, and/or are they to be required of others? How would a marine terminal operator know that a container arriving into it was supposed to have a CSD on it to be read? Why would port facilities install such a global reading infrastructure if the devices are not required by the government?

Further, there has been no discussion with industry of the necessary protocols for how to address anomaly readings or alerts that would be generated from CSDs, or how governmental authorities would be involved in addressing the tens of thousands of anomalies resulting from CSDs reporting that a container’s door had been opened.

It is not appropriate for standard setting to precede discussion and resolution of such issues.

## **7. Security Concerns Regarding “CommerceGuard”**

The “CommerceGuard” device has the ability for persons to change or write new information into it. A security vulnerability is created in a device when parties can amend or write new information into it. The security vulnerability arising from the ability to write new information into a container security device has been identified repeatedly, but has not been publicly addressed or resolved by GE and its business partners. The industry has been sufficiently concerned about the security vulnerabilities such a “write” capability poses, that the ISO standard specifically precluded “write” capability in the ISO RFID container e-seal standard.

## **8. Product Marketing vs. International Standard Setting**

While no international standard setting process is without its shortcomings, the ISO is generally recognized as the appropriate non-governmental international standards setting body. GE and its business partners know this and have followed the ISO RFID container device standard setting process closely. They not only have insisted that the ISO standard does not apply to their CSD device, they have consciously avoided asking the ISO to establish an international CSD standard.

ICSO representatives have stated that the ISO is not capable of producing a standard in a timely manner. That is simply incorrect.

Until governments have discussed and agreed upon what the requirements of a CSD should be – hopefully pursuant to a structured dialogue with the industry, it would be premature to undertake an initiative to develop an international standard for such undefined devices; however, should governments define and agree on CSD requirements, there is no reason why the ISO could not develop an international standard for CSDs.

The industry certainly does not wish to prejudge the work product of the proposed ICSO process. However, the industry cannot help but perceive that an effort created by GE and its business partners to establish a new organization that will propose international standards that they wish to be applicable to their product, after those parties have refused to contribute constructively the ISO e-seal standard setting process and refrained from seeking an ISO standard “container security devices” that would apply to their type of product, might reasonably be interpreted as a way to promote a product in which they have a proprietary, commercial interest.

There has been no satisfactory justification for why container owners, container users, the world’s port industry, or governments should find value in one set of technology developers establishing their own new organization to develop container security technology standards.

## **9. Final Comment**

Based on the Council's experience and on its Member carriers' discussions with shippers, there appears to be little interest in or benefit to commercial shippers or carriers from an RFID "container security device". We are not aware of significant commercial shipper interest by shippers in such devices for supply chain management purposes.<sup>2</sup> Writing cargo shipment information into an RFID device that is to be affixed to a container is not something in which carriers or their customers have expressed significant interest.

The potential definition and value of a CSD as a security tool remains an unresolved issue.

An RFID device that does not impede entry but only records whether one, or perhaps either, container door has been opened, and only provides that information when read by a geographically fixed reader, would appear to provide questionable additional security benefits, but would add costs of hundreds of millions of dollars per year if broadly deployed.

As container seal anomalies have demonstrated, such a device would capture the fact that container door openings occur, most commonly caused by customs authorities inspecting the shipment, or by anomalies resulting from data input errors.

Neither a container seal nor a CSD, as presently understood, is going to provide true insight about what is actually in the container.

Technology vendors appear to be struggling with the fact that there is little commercial interest in an RFID container device, and the fact that, at least as RFID CSDs are presently understood, there is marginal, if any, security benefit, but substantial cost and infrastructure obstacles. Accordingly, at least some of these vendors now appear to be arguing that a CSD should be seen as an automated conduit of various, undefined data elements that can be inputted into their devices, captured by their data systems, and then fed into the U.S. Department of Homeland Security's "Secure Freight Initiative" concept.

There is so little definition, understanding or agreement on what a U.S. "Secure Freight Initiative" might be, what data it would need or use, how it would be populated with information, or whether it would be internationally accepted, that the role of CSDs in such a concept is not presently evident. It is also not evident, even if CSDs were considered in such a capacity, whether they would be the most appropriate way to obtain the desired data. What is evident is that such a role for CSDs is undefined, is not agreed to, and would face many significant issues.

---

<sup>2</sup> Whether devices based on satellite technology, which does not require a global network of fixed readers in order to identify the location or status of a container, could meet certain shippers' commercial needs more effectively is not an issue addressed by these comments.

The World Shipping Council and its Member carriers fully support new security initiatives and new security technologies designed to advance clearly understood and well founded security strategies.

For example, the industry understands and accepts the security strategic decision by the U.S. and other governments that preventing and detecting the possible containerized transportation of unlawful nuclear or radiological material is the number one container security priority. Accordingly, the industry is working with U.S. governmental authorities to ensure that all containers are screened for radiation, and understands and support the U.S. government's deployment of new generation of radiation detection equipment through the Advanced Spectroscopic Portal (ASP) program, the Container Security Initiative (CSI), and the U.S. Department of Energy's "Megaports" program.

For example, the industry supports the strategy of cargo risk assessment and targeting before vessel loading, and fully supports governments going beyond current cargo shipment data collection to require more relevant shipment information before vessel loading, so that targeting efforts know the identify of the parties buying and selling the goods, the origin of the goods, the identity of the business that loaded the container, and the name of the consolidator that may be involved.

For example, the industry fully supports the strategy of further piloting and examination of whether a container screening system, involving radiation and non-intrusive cargo density screening of all containers prior to their being loaded onto a vessel can be implemented in an effective international manner – because such a capability would help governments answer the most important container security question: "What's in the box?"

ICSO and similar efforts may be understandable as product marketing initiatives; however, RFID CSDs lack well defined and agreed government security objectives or concepts of operation. They do not tell you what is in a container and are unlikely to impede or detect the unlikely, but potential, terrorist use of a container. RFID CSDs lack a significant commercial value or acceptance. They would involve substantial cost for an arguable security benefit. They would require a huge global network of readers that would need permission to be installed, operated and maintained on the premises of thousands of facilities owned by numerous different parties in numerous different countries. They lack any sort of agreed international protocol for who would read the devices, who would act on the data generated, or who would own and control or have access to the data generated.

If such devices are to be seriously pursued by the government as an element of container security strategy, an open and careful examination of these issues should be conducted with the affected sectors of industry. Should such a process produce agreed clarity on the applicable security requirements and how such devices would meet them, then development of appropriate international standards by an appropriate standards setting body would make sense.