

Introduction to CSOS Auditing

American Society for Automation in Pharmacy (ASAP)

Annual Industry & Technology Issues Conference

Jan. 20-22, 2005

This document prepared and facilitated by:

DRUMMOND GROUP INC.

<http://www.drummondgroup.com>

Continuing Education Objectives

At the end of the introduction to CSOS Auditing:

1. You will have gained a basic introduction to what is being audited and the impact it will have in helping organizations select product(s) that best fit the needs of the supply chain.
2. You will know who needs to be audited.
3. Your organization will know what to look for in a certifying organization to ensure an unbiased view of certified products.

In addition, you will learn more about long-term CSOS interoperability strategies that include auditing for regulatory compliance, conformance to standards and interoperability between software products.

I. Overview

The Controlled Substances Ordering System (CSOS) is an electronic commerce initiative overseen by the U.S. Drug Enforcement Administration (DEA) which provides an automated alternative to the current paper-intensive process controlling the purchase and distribution of Level I and II controlled substances.

In the current paper-based process, paper forms must be created or updated at every registered shipping location when controlled drugs are transferred. With CSOS, the DEA is defining a system based on digital signatures which allows for the paper forms, known as Form 222, to be replaced by digital messages often referred to as e222 or electronic 222 forms. Purchasers and suppliers may now use either of these methods, paper-based or electronic forms, to fulfill DEA requirements that prevent illegal diversion of controlled drugs.

The DEA proposed rule for CSOS includes technical and business requirements for products used to digitally sign, transmit or receive E222 forms. Software companies that provide these products must participate in an initial audit of the product and additional audits when changes are made to the core digital signing technology. End user companies that build in-house CSOS systems for digital signing, transmission or receipt of e222 forms also must be audited.

Drummond Group Inc. (DGI) will provide CSOS Auditing services such as delivering certification for software products-with-version in compliance with DEA rules. CSOS Auditing Certification is proof that software offerings can enable purchasers and suppliers to interchange e222 forms in a predictable and secure manner compliant with DEA requirements.

In addition, DGI will continue to promote long-term interoperability of CSOS and related systems by working with the software vendor community and end-user corporations to combine DEA requirements with recommendations from industry consortia such as the HDMA to promote implementation of CSOS-compliant production systems.

II. What is being audited?

1. Confirmation that products-with-version have been issued seals of compliance to FIPS (Federal Information Processing Standards). FIPS sets best practices and prescribes specific computer software algorithms approved by the federal government to insure data security.
2. The ability to digitally sign, transmit and receive e222 forms in a FIPS enabled mode. Auditing will confirm that the products can perform digital signature functions while using only FIPS required methods.
3. The ability of products to execute fundamental digital signature processing including applications of digital signature, validating a business partner's digital signature using that business partner's public key and validation of message integrity.
4. The products' ability to recognize and act on invalid digital signatures and invalid digital certificates that have expired or have been revoked by the DEA.

III. Who needs to be audited?

The proposed rule requires that systems developers or vendors must be audited. If you are developing an in-house system that digitally signs, transmits or receives e222 forms, your system must be audited. If you are purchasing a product that digitally signs, transmits or receives e222 forms, the software vendor that provides the system must be audited and provide you with proof of certification for that product-with-version.

For both systems developers and vendors, an additional audit is required whenever signing or verifying functionality is changed.

IV. What to look for in a certifying organization

The certifying organization should have experience in testing and auditing security related software standards, in particular the use of digital signature technology.

To remove the likelihood or appearance of biased auditing, certifying organizations should be verifiably neutral companies that do not themselves produce or market CSOS products and do not have business partnerships with companies that produce or market CSOS products.

The proposed rule requires the use of an independent, third-party in section 1311.60: *"For systems used to process orders, the system developer or vendor must have an initial independent third-party audit of the system and an additional independent third-party audit whenever the signing or verifying functionality is changed to determine whether it correctly performs the functions listed under paragraphs (b) and (c) of this section. "*

V. Long-term strategies for CSOS enablement

As more and more organizations begin to use CSOS, the need for interoperability will grow. Increasingly more systems developed separately by different software vendors will be exchanging CSOS orders and related transactions. It is important to accommodate the needs of such a diverse group by providing choice from a wide array of software solutions providing the same underlying technology, but with different bells and whistles and corresponding price points.

The current DEA rules require software products to be audited. But the DEA has not, and likely will not in the future, make requirements concerning the exact message format, the exact transport method or describe exact business process models for the exchange of e222 forms. De jour standards or common practices may arise from the marketplace or will be driven by industry consortia. For example, the Healthcare Distribution Management Association (HDMA) has recommended the use of AS2 EDI-INT (Applicability Statement 2 for EDI over the Internet) as the common transport method and ANSI X12 850 formats as the common message formats for CSOS-related transactions.

AS2 is a secure business-to-business communications standard which can transport any type of message (including EDI and XML) currently used in the retail, consumer product goods (CPG), Hardlines and financial services industries. There are currently more than 30 commercial off-the-shelf interoperable AS2 products providing a wide range of price points and functionality to serve any industry. (See <http://www.drummondgroup.com/html-v2/as2-faq.html> for more information.)

DGI plans to continue working with all CSOS-related stakeholders to drive adoption of high quality, interoperable CSOS solutions. As a first step, DGI plans to include testing of FIPS certified and enabled products in the next round of AS2 interoperability testing.

You can help by engaging with industry consortia to define common business and technical practices for e222 message format, message transfer and business process.

Learning Assessment Questions

- 1. What is CSOS?**
- 2. What is CSOS auditing?**
- 3. Who has to be audited?**
- 4. What is the importance of CSOS auditing?**
- 5. What are the long-term strategies to enable CSOS interoperability?**

Answer Key

1. What is CSOS?

The Controlled Substances Ordering System is a DEA electronic commerce initiative that provides an automated alternative to the current paper-based process of controlling the purchase and distribution of controlled substances. With CSOS, paper forms are replaced by electronic forms commonly referred to as e222 and physical signatures are replaced by digital signatures.

2. What is CSOS auditing?

The DEA requires that applications used to digitally sign, transmit and or receive CSOS orders are audited. The audit covers a subset of the proposed rule requiring that products are Federal Information Processing System (FIPS) certified, that digital signature functionality works in FIPS enabled mode and that products can recognize and act on orders whose digital signatures or digital certificates are invalid.

3. Who has to be audited?

Software companies that sell CSOS products are required to participate in an initial audit of their products and additional audits when core digital signature technology is changed. End user companies that build in-house CSOS systems also are required to be audited.

4. What is the importance of CSOS Auditing?

The DEA requires that any applications used to digitally sign, transmit and/or receive CSOS orders must be audited.

5. What are the long-term strategies to enable CSOS interoperability?

The DEA has not and likely will not in the future make specific requirements concerning exact message formats, exact transport methods or exact business process models for the exchange of e222 forms.

As the pharmaceutical industry begins to utilize CSOS, the need for interoperability will grow. These needs can be addressed through participation in the creation of common practices through industry consortia and through ongoing interoperability testing of common technologies as they are identified.

Additional Information

For more information about CSOS, please visit the DEA website:

<http://www.deadiversion.usdoj.gov>

For more information about DGI testing, please visit:

<http://www.drummondgroup.com>

FAQs on AS2 and Interoperability may be found at:

<http://www.drummondgroup.com/html-v2/faq-retail-as2.html>

About Drummond Group Inc.

Drummond Group Inc. (DGI) is an independent, privately held company that works with software vendors, vertical industries and the standards community to drive adoption for standards by conducting interoperability and conformance testing, publishing related strategic research and developing vertical industry strategies. Founded in 1999, DGI represents best-of-breed in the industry on linking horizontal infrastructure technologies, standards and interoperability issues with the needs of vertical industries such as retail, grocery, health care, transportation, government and automotive. For more information, please visit www.drummondgroup.com or email: info@drummondgroup.com