clearswift
A HelpSystems Company

Improving Control of Regulated ITAR Information

The United States Government has substantially increased action against organisations and individuals responsible for breaches of the International Traffic in Arms Regulation (ITAR). This poses challenges for global defence corporations as data related to specific technologies may need to be transferred over the internet, or stored locally outside of the United States, in order to make business processes flow smoothly.

Products

- Clearswift SECURE Email Gateway (SEG)

Professional Services

Consultancy options are available to help with the deployment and configuration of this solution:

- Architecture Design
- Policy Design
- Solution Implementation

Support

Clearswift provides 24x7 global support as standard, with additional options for an Advanced or Premium support service.

Business Problem

As an important USA export control law, the International Traffic in Arms Regulations (ITAR) affects the manufacture, sale and distribution of technology in the defence sector. The goal of the legislation is to control access to specific types of technology and their associated data. Overall, the US Government is attempting to prevent the disclosure or transfer of sensitive information to an unauthorised foreign national.

ITAR can pose challenges for global corporations, since data related to specific technologies may need to be transferred over the internet or stored locally outside of the United States in order to make business processes flow smoothly. The responsibility lies with the manufacturer or exporter to take the necessary precautions and steps to certify that they are, in fact, meeting ITAR compliance requirements.

Failure to comply can result in heavy fines, having to spend funds on remediation, compliance measures and may also require the party to submit to external audit. As a result, effective management of sensitive ITAR information becomes key in order to remain competitive and a trusted supplier.

Supporting ITAR compliance with Clearswift

Data security will have different requirements for a commercial company, but there is a myriad of best practices that Defence organisations must to follow in order to appropriately secure ITAR data:

- Define and maintain an information security policy
- Build and maintain a secure network by installing and maintaining network defences to protect sensitive data
- Protect sensitive data with encryption
- Regularly monitor networks
- Implement strong access control measures
- Track and monitor access to network resources and sensitive data

Whilst this list is not exhaustive, it does highlight the need for an advanced solution that can 1) detect ITAR information, and 2) ensure it is adequately protected as it flows between teams within the organisation, and across the external boundary.

Clearswift provides a holistic cyber security platform that enables sensitive ITAR information to be identified and tracked as it flows through email. The platform, to include a set of optionally deployed components, seamlessly integrates with existing information security systems to enable improved ways of working, enhanced sensitive information security and visibility of information flow.

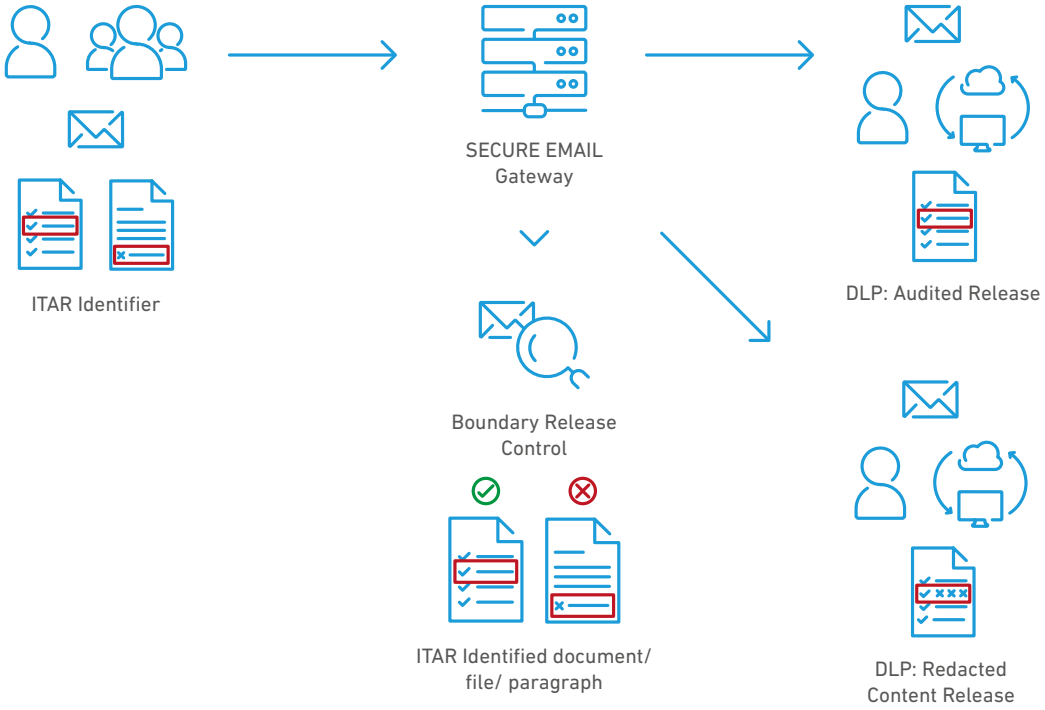
With email still being the primary business collaboration tool, defence organisations need to ensure that the ITAR content and information they send and receive is permitted to enter or leave the organisation.

ITAR protection with the Clearswift SECURE Email Gateway

The Clearswift SECURE Email Gateway (SEG) helps to secure against ITAR data breaches, protecting the organisation and ensuring compliance with the current regulation. The Clearswift Secure Email Gateway (SEG) will:

- Scan emails for sensitive ITAR content – both inbound and outbound (as a compliance breach relates to both scenarios)
- Offer granular organisational policy to provide the necessary flexibility to permit multiple behaviours, depending on the senders and recipients of the message
- Provide logical segmentation of communication of sensitive information inside the organisation, without the need for segregated email solutions (using the Clearswift SECURE Exchange Gateway option)
- With the Adaptive Redaction functionality, allow for content to be dynamically modified (redacted or sanitised), allowing the rest of the communication to be delivered. This ensures secure but continuous collaboration, rather than having to 'stop and block' emails and force a remediation against a potential ITAR breach.
- Through Policy, apply encryption where required.

Clearswift Solution for Improving Control of Regulated ITAR Information



Solution: Boundary controlled release. Fully audited information control.

Features

Designed to meet small, medium and enterprise scale deployments, the Clearswift SEG provides:

- business operation level information asset protection – focused on the asset value, risk profile and the associated impact of the data associated with it,
- secure handling of ITAR information that is shared through email systems,
- deployment on-premise, or in the cloud, with hybrid deployments possible,
- granular control based on content and context as required to meet the policy requirements,
- recognition of classification tags and/or enforcement of tags before information can be shared,
- multiple encryption options to support different communication policies including TLS, PGP, S/MIME and Portal-based encryption,
- advanced options for dealing with scanned documents and image files (Optical Character Recognition and image-based text redaction),
- advanced Anti-steganography functionality to prevent infiltration of malicious code, or exfiltration of sensitive information in images,
- coherent and consistent sharing of information within and across teams both internally and externally to the organisation that are holding or creating the data in support of the need for collaboration across multiple organisational and security domains,
- full compatability with Microsoft Office 365,
- necessary controls and visibility of inbound/outbound data flow to support both audit and compliance under the specific collaboration policy requirements for ITAR,
- support for operational requirements for cyber security monitoring and incident response,
- support for multiple implementations of encryption that are common to the UK and international Defence communities.

Benefits

Designed to scale for organisations of all sizes, the Clearswift SEG solution offers:

- **Low friction:** low friction, seamless deployment using an established, proven and assured security technology platform to minimise cost and maximise time to value.
- **Deep content validation:** proven capability to meet the specific demands of detecting ITAR related content, especially in the ability to implement controls requiring deep content inspection checks, validation of information sensitivity and the adaptive requirements for content modification for an effective ITAR policy.
- **User experience:** innovation-led improvement to end user experience for secure sharing of information that reduces risk and the associated impact of an ITAR compliance breach.
- **Reduced operational cost:** specific features to deal with policy violations to minimise operational costs.
- **Support:** underpinned by a defence-aware organisational culture that is creative, passionate and built around a customer focused 'one-team' approach, aligned with the essence of the Team Defence community, to ensure the low-risk delivery of enhanced protection.

About Clearswift

Clearswift is trusted by organisations across the globe for advanced content threat protection and the highest level of defence against breaches through today's digital communication channels. Our technology supports a straightforward and 'adaptive' data loss prevention solution that gives teams the freedom to securely collaborate, whilst providing information security personnel with visibility and control of sensitive information flow.

Over 70% of Clearswift clients operate within critical national infrastructure, including defence conglomerates, government agencies and financial institutions, all of which demand the most advanced cyber threat prevention and information security solutions. Working closely with these clients over two decades has enabled Clearswift to gain a clear to understanding of the cyber challenges they face, keep abreast of their evolving threatscape, and support compliance with the complex regulatory environment within which they operate.

Our united approach to working with clients has ultimately driven the specialised development of the award winning Clearswift product portfolio which is backed up with a superior 24/7 customer and partner support service, and an extensive channel partner network across the globe.

To learn more about Clearswift, visit **www.clearswift.com**

Contact Us

Clearswift Ltd.
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire RG7 4SA
United Kingdom

E: info@clearswift.com

T: +44 118 903 8300

Deployment

The Clearswift SECURE Email Gateway is designed with flexibility in mind. The solution can deployed as a stand-alone solution, in conjunction existing security solutions or together with other Clearswift products which form the Aneeysa platform. When deployed with other Clearswift products, a consistent Deep Content Inspection (DCI) and policy engine ensures the uniform discovery of critical information, DLP policy and Adaptive Redaction functionality for consistent information security management. The Clearswift portfolio includes:

Clearswift Information Governance Server: enables users to securely register and classify information with the IG Server. Compliance Officers are given access to oversee who and what is being registered as well as the ability to track, trace and control information (not just files) passing across the organisation boundary, in real-time, including information provenance reporting.

Clearswift SECURE Web Gateway: offers granular control over what users can access or share online. Flexible, policy-based filtering and content aware inspection extends beyond limiting browsing, to view inside HTTP/S encrypted traffic to prevent phishing and malware attacks and the unauthorised exposure of sensitive information.

Clearswift ARgon for Email: augments existing email security gateway infrastructure to enable Adaptive Redaction functionality and the ability to track and control sensitive information contained in email crossing over the organisation's boundary (inbound/outbound).

Clearswift SECURE Exchange Gateway: enables data loss prevention policies to be applied to internal email communications, along with the ability to track and control internal information sharing and email segregation functionality without the need for separate infrastructures.

Clearswift SECURE ICAP Gateway: designed to co-exist with an existing web security solution, the Clearswift SIG enables Adaptive Redaction functionality, and the ability to track and control information passing through an ICAP compliant web gateway or solution, including Managed File Transfer (MFT), cloud storage and collaboration applications.

Cost

Flexible pricing options are available to suit differing implementation requirements across the varying scale of organisations that constitute the defence community. This ensures the solutions are commercially appropriate, affordable and sustainable whilst offering the ability for customers to consolidate their existing security solutions into an integrated platform for both on-premise and cloud delivered services.