FORTRA

**GUIDE** *(Clearswift)*

# Securing Government Data

*With nation-state attacks on the rise, and cyber criminals more targeted, professional, and motivated than ever, governments around the world have become dependent on cybersecurity solutions to stay ahead of the latest threats.*

*But with government departments holding valuable data on its citizens, it’s vital that they use a solution that can defend themselves against attack and keep that data safe and secure.*

## The Cybersecurity Risks for Highly Regulated Organizations

Email remains the most popular way to communicate and share data, and it's why many cyber attacks target email. There is no failsafe solution for defending against cyber attacks, and there are many ways that a hacker can use email to gain access to an organisation's data. This makes cybersecurity an ongoing and growing challenge for almost every industry.

Cyber attacks are so coordinated and intentional now, that's any CISO would rightly be nervous of the damage they could cause. But for organisations that hold sensitive and therefore, valuable data in the world, the pressure is immense. Industries such as finance, critical infrastructure, and government need email security solutions that they know will protect them.

When it really hits home for highly regulated industries, is in the aftermath of an attack. Because the data is so sensitive, the fallout from a breach is far more severe than in less regulated industries. For example, in February 2022 the UK's health service the NHS was the victim of an attack. Personal information and the medical details of thousands of patients were leaked. Not only was this a breach of General Data Protection Regulation (GDPR) but such an incident can erode trust between citizens and government and could even lead to identify theft.

In this guide, we will take a deeper look at regulations, threats, and the solutions needed to protect government departments.

## Who Do Regulations Affect?

The need to protect data isn't the only reason governments require robust email security solutions. Compliance can be just as important. There are a wide range of data privacy regulations that can be applied depending on the level of government, location of government, and the information stored.

GDPR is one of the most well-known data privacy regulations. While it is an EU law regulating data protection, it affects any organisation that stores and manages data relating to EU citizens. The fines for failing to comply with GDPR can be in the millions.

There is similar data regulation in other countries around the world. Australia was one of the first countries to align its privacy laws with changes brought about by the digital revolution. It amended its 1988 Privacy Act The Privacy Amendment (Notifiable Data Breaches) Act 2017 to introduce concepts and requirements adopted by the GDPR the following year.

While the US has no country-level equivalent there is the California Consumer Privacy Act (CCPA), which protects the personal data of consumers residing in the state of California.

Of course, government contracts around the world can have even higher standards for partners looking to work with different agencies and departments. Failure to meet these standards can result in a loss of contract or even rejection of consideration for future contracts. Understandably so any organisation is only as secure as its weakest link and if a government supplier has lax cybersecurity, that can affect the department it works with.

More than ever before, governments worldwide are prioritizing the implementation of cybersecurity measures to combat the growing threats. This is leading to the creation of more regulatory standards for government data.

## The Journey of Data

The sharing of information within any organisation is mostly performed digitally. Government is no exception, with digital communications flowing internally with multiple levels of clearance, and externally with outside agencies, consultancies, partners, and citizens.

Understanding what data flows through the organisation and who handles and receives the various types of data is a central component in creating a data loss prevention policy. Not knowing where all data especially sensitive data lives and flows is a major vulnerability to any organisation, and vulnerabilities are lucrative to cybercriminals. On some occasions a government department will be at a local level communicating with citizens to make online payments, and therefore holding financial data. At other times it will be storing social security details, and in some extreme cases such as defence there is highly confidential data everywhere. Knowing what all this is and where it is stored is one of the most important steps in keeping it secure.

### Inbound and Outbound Data

Email is the primary way to send information quickly and resourcefully. As such a ubiquitous tool, email also remains a primary target for cyber attacks. Government departments need to make sure emails coming into the organisation are safe from malware and other advanced threats such as phishing, spyware, ransomware, and internal data loss risks. While some of the threats lurking in emails can come from unknown sources, some come disguised as a trusted outside partner. While government departments impose very high standards on their external partners, that does not make it impossible for the partners to be digitally compromised.

### The Internal Threat

While many deem outside threats coming into an organisation as the most likely, just as critical are the internal threats. Sharing information digitally can save time, but if someone is accidentally added to the email, it can become a data breach. It doesn't make a difference if the recipient is internal or external, sensitive data has potentially been exposed.

Levels of clearance in an organisation may be the most apparent in government. Classified information is not intended for all eyes, that's why it's considered classified. Therefore, many government departments need a security solution that understands the complexities of classified information flowing inside the many levels of government. been exposed.

## Creating the Policy

The goal of email security solutions should always be to protect the organisation's data. Once that data is identified and understood, the policy needs to be created. An email security solution that's easy to deploy, monitor, and manage will help support and enforce a policy in a way that doesn't burden the IT department, email administrators, or messaging teams. Features such as the ability to handle all threats from a single interface and have employees manage their own quarantine list will help increase the efficiency of the solution and ultimately free up time for IT teams to spend on other projects.

The following steps can guide any government department to email security best practices:

1) **Determine what data needs protection** – Compliance regulations dictate that sensitive data such as Personal Identifiable Information (PII) and payment details are safeguarded from unauthorised disclosure. A solution that can detect and remove unauthorised sensitive data from incoming and outgoing emails, and automatically encrypt any authorised data, will protect employees and the organisation if sensitive data is incorrectly sent or received.

2) **Identify cyber threats** – The right email security solution must prevent malware, spyware, ransomware, BEC (phishing) emails, unwanted data acquisition, and unnecessary file types from reaching inboxes.

3) **Establish a robust and sustainable email security policy** – An email security solution that's easy to deploy, monitor, and manage will help support and enforce a policy in a way that doesn't overburden the IT department, email administrators, or messaging teams. Features such as the ability to handle all threats from a single interface and have employees manage their own quarantine list will help increase the efficiency of the solution and ultimately free up time for IT teams to spend on other projects.

4) **Close the zero-hour window** – Anti-malware solutions are great for defending against known dangers. But what happens if a brand-new virus tries to enter a network before security loopholes have been identified? The Sandbox, an email security solution, filters and analyses the content of messages and attachments. If the content contains a threat, the Sandbox will sanitise these evasive threats thereby helping to close the vulnerability.

5) **Encrypt sensitive data** – To aid compliance, email security solutions need a range of easy to use policy based encryption options including TLS, Web-portal, or password-protected messages.

6) **Monitor traffic behavior and performance** – Visibility of emails and comprehensive reporting is important when determining and enforcing policy. Email security solutions that provide detailed audit trails help IT teams investigate potential breaches. Those that export data to SIEM systems allow organisations to get a 360-degree view of the data that flows in and out of it.

7) **Education** – An organisation's employees are some of its strongest defences in email security but keeping them vigilant won't happen overnight. Having a stable email security education programme to teach people how to stay alert about their inboxes and correspondences is key.

Creating an email security policy that understands content and context is vital for strong threat protection.

## Critical Data Needs Email Security

Clearswift solutions offer an unprecedented level of flexibility and granularity in policy deployment and control. Clearswift Secure Email Gateway (SEG) uses traditional signature, heuristic, and cloud-assisted lookups to deliver protection against malware, ransomware, and spyware. SEG's Deep Content Inspection (DCI) can detect active code in files and allows the organisation to manage how to handle any violations.

### Sanitizing and Redacting – Better Content Safeguarding

SEG can detect information that shouldn't be there. The data might be deliberately exfiltrated or someone could be sending out some content that may contain hidden classified information.

Through Structural Sanitization, the SEG can clean content to ensure that no sensitive data is being exfiltrated either deliberately or accidentally. Documents can have sensitive or offensive text automatically redacted. Even images within documents can have sensitive content redacted from the image and then replaced in the document. Document properties (metadata) can be cleaned; for example, agencies may want to remove the "Author" name from all publicly available documents.

Clearswift's Anti-Steganography rebuilds images to remove any data added by steganography tools, which is often missed by other email security solutions such as Microsoft Office 365.

With URLs being used as a key method of attack, any found in messages and attachments are checked in real-time to see if they relate to malicious, phishing, or spam campaigns. Messages can be blocked. URLs are sanitized or rewritten to use Time-of-Click services.

### Encryption that Keeps Government Moving

To provide automatic security and regulatory compliance, SEG features encryption. This allows policies to be based on sender, recipient, subject, message body, attachment types, attachment content, message header, or document metadata.

By providing multiple options to send data securely, organisations can choose the best method to deliver content to third parties in the most appropriate method. The following are various encryption methods used by SEG:

***Transport Layer Security (TLS)***

This mechanism is used to secure messages over the internet between servers. It is completely transparent to end users and is therefore widely used.

***Password protected files***

This method wraps the sender's message and attachments into a password protected Zip file or PDF which is then delivered to the recipient. The sender must get the password to the recipient, typically using a different medium such SMS, or email to a secondary email account.

***Web Pickup Over SSL***

The hosted email portal allows senders to send messages to recipients using a webmail style mail client and respond to the sender in a secure fashion. This is typically used for low volumes of message transaction to users of all levels.

| Method | Usage Frequency | | Recipient | | Level of security |
|---|---|---|---|---|---|
| | Regular | Adhoc | Business | Consumer | |
| TLS | Y | Y | Y | Y | Over Network |
| Password | Y | Y | Y | Y | To User |
| S/MIME & PGP | Y | | Y | | To User |
| Web Portal Pickup | | Y | Y | Y | To User |

## Securing Classified and Unclassified Data

The words "classified" and "unclassified" are synonymous with government departments. The data for classified and unclassified information needs to move differently inside of government. Not all eyes are cleared to see classified documents whether digital or not. Naturally, a security solution is needed to keep digital classified information guarded. Clearswift's email and web products have pre-configured, standard lexical expressions. When it comes to other specific values that need detecting, lexical expression qualifiers (LEQs) are used to validate "true" information found against external data sources such as a database. Logic can be added for the "if this, then this" scenario.

This is important for government departments, when sharing classified information between approved colleagues. For example, if coworkers in the defence department are sharing highly classified military strategies, the data should always be encrypted. To ensure the data is encrypted, it is inspected for attributes that identify key terms. Clearswift can import a snapshot of specific details for official use or top-secret correspondents. The LEQ file is then indexed and hashed for security. The more information verified through LEQs, the more the system can be sure of a policy match and automatically apply the appropriate action, reducing the amount of manual intervention required.

## Sending File Transfers Securely

Government departments rely on the ability to share files daily with their citizens. This is true in many forms of governmentincluding local government where tax departments, law enforcement, and payment processors need to share files to keep business moving. Clearswift Secure ICAP Gateway (SIG) is a fully automated solution that augments the security of critical information flowing through an organisation's existing web proxy infrastructure or managed file transfers.

Going beyond traditional stop and block technology, SIG applies the appropriate measures to questionable content based on the government department's policies to allow safe content to flow through and reduce disruptions.

SIG integrates seamlessly with Secure File Transfer platforms to create a powerful solution for government departments that require enhanced security around file transfers. A file transfer solution with security and compliance features has never been more crucial than now, with hybrid working environments and bigger reliance on digital procedures rather than old-fashioned paperwork.

## Clearswift Stands Above the Rest

Managing cybersecurity for any organisation is complex and even stressful at times and having solutions that don't get in the way while keeping organisations secure alleviates many burdens. Clearswift can also be deployed alongside many other systems for a robust layered approach to cybersecurity that fills the vulnerabilities left by a sole solution.

Clearswift is highly configurable giving government departments the ability to apply very granular policies to data. Not all departments are the same, and policies should reflect the level of government they are securing. Whether protecting the PII of its citizens or military information to protect millions, Clearswift protects data from the point of creation and throughout its journey.

## Ready for data security help without hassles?

Contact Us

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.