FORTRA

Federal ITAR Solution

The Threat Landscape

In an ever-changing threat landscape, federal agencies are struggling to strike the balance between prioritizing mission-critical objectives and creating a robust security environment to combat threats.

Agencies that still take a perimeter-only approach to their data security are increasingly vulnerable to security breaches, primarily because the perimeter, as we knew it, no longer exists. Today's government entities need to share data in a variety of ways, with a variety of people, to efficiently collaborate and conduct multi-faceted missions. This data exchange is happening in complex, often hybrid IT environments at an unprecedented pace, not to mention in a world of growing cyber-attacks and threats. Human error, workflow bottlenecks, cumbersome systems, and a lack of system integration can leave federal agencies, and the information they need to protect, vulnerable.

All of these factors introduce the risk of sensitive information getting into the wrong hands either intentionally or by accident, creating a substantial impact on the economy, on citizen's lives, and their trust in their government.

Government agencies must take a proactive approach to their information protection and strike the fine balance between securely protecting vitally sensitive data and sharing essential information and collaborating with their trusted partners.

A Proven Security Leader

Security is a collaborative process, and Fortra is your trusted partner. As part of our purpose of helping you Build a Better IT™, our goal is to make your IT security more powerful. We deliver the tools and flexibility you need to keep your mission-critical projects running smoothly in an ever-changing threat landscape with security at the forefront.

Our technology is best-of-breed, and simple to deploy and manage. Globally, government and civilian organizations alike use layered Fortra solutions to attain high-level business objectives and stay secure, including:

- National defense
- Defense intelligence
- Federal agencies
- Civilian partners

Fortra takes a Zero Trust approach to securing mission-critical data, addressing the many challenges of data security. Regardless of how it moves or where it lives, data is identified, secured, and protected throughout its journey, ensuring stringent security requirements are met.

Data Classification:

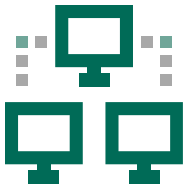
Identify and prioritize the specific types of data you need to protect most, including unstructured data. Classification streamlines the load when it comes to handling data, as well as enhances security and compliance. Your investment in security applications pays off with an added layer of security protection and awareness around sensitive data. Our classification solutions offer essential management and control of your data to minimize risk.

Data Loss Prevention (DLP):

Minimize the risk of a data breach by automatically removing or redacting sensitive data from emails and documents as they are sent or transferred to and from the cloud. Adaptive DLP applies an additional layer of real-time sanitization to protect from phishing, ransomware, and other Advanced Persistent Threats.

Email Security:

Real-time sanitization is applied to confidential or highly sensitive data leaving or entering the organization to protect from malware, ransomware, and other Advanced Persistent Threats that can be delivered through phishing emails or business email compromise attacks. Email security not only controls who can share confidential data, it also provides protection from email-based cyber attacks ensuring that any emails sent and received are safe to open and click.



Secure Managed File Transfer (MFT):

An automated managed file transfer solution provides a secure and compliant way to share data, all through a centralized, dashboard-style platform. With the addition of our Adaptive DLP and anti-virus abilities, you can ensure that files sent and received do not contain any sensitive data, as sensitive data is redacted from delivered file exchanges.

Data Encryption:

Encrypting data at rest and in motion is a vital piece of any data security ecosystem and is your last line of defense to ensure your sensitive data does not fall into the wrong hands. Our encryption solutions can substantially limit the impact of a data breach as the data cannot be decrypted without the appropriate key.

Digital Rights Management:

Automatically secure sensitive data as it is shared externally with suppliers and partners, while also tracking successful and unsuccessful access to your sensitive data. Fortra Digital Rights Management allows administrators to revoke access to sensitive data, such as financial or legal records, at any point.

Our Data Security Suite in action: ITAR use case

A defense contractor needs to share large files with a variety of third-party suppliers, some of whom are authorized to receive International Traffic in Arms Regulations (ITAR)-related information, while others are not. Applying layered data security solutions can help ensure that highly confidential ITAR information does not land in the wrong hands, both while it's in motion and while it's at rest.

Protecting the digital assets of ITAR information such as plans, diagrams, photos and other technical data requires layered security measures be in place to ensure compliance mandates are met to help restrict access.

1

Understand And Classify

The foundation of a solid data security strategy begins with data classification. A data classification solution helps you identify and prioritize the data you need to protect, including critical unstructured data that could very well be ITAR-related. Our classification solutions offer essential management and control of your data to ensure compliance.

ITAR
International Traffic in Arms Regulations

2

DETECT AND PREVENT

Minimize the risk of a data breach by automatically removing or redacting sensitive data from emails and documents as they are sent or transferred to and from the cloud. Adaptive DLP applies real-time sanitization of confidential or highly sensitive data to protect your organization from phishing, ransomware, and other Advanced Persistent Threats. Email security helps protect ITAR-related information from phishing and business email compromise (BEC) attacks through robust phishing defense, response, and brand protection capabilities.

3

SECURE AND PROTECT

Our secure managed file transfer solutions can secure and protect ITAR data through its entire lifecycle, everywhere it travels, no matter its size, who has it, or where it's stored. We help you protect confidential data at the point of its greatest vulnerability— when it's being used by others, and while it travels outside your perimeters into unmanaged domains, devices, and applications. We do this by attaching encryption, security, and policy directly to the data itself, giving security practitioners and IT teams the power to control it, no matter where it goes.

Digital Rights Management further secures this ITAR-related data by tracking, auditing, and revoking access if required.

Our Data Security Suite in action: ITAR use case

NORTHROP GRUMMAN

BAE SYSTEMS

GENERAL DYNAMICS

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.

fta-corp-gd-1022-r1-79d