WHAT IS DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC), is an email authentication policy and reporting protocol designed to detect and prevent email spoofing.

Organizations using DMARC can specify what happens to inbound unauthenticated email messages (e.g., allow, quarantine, reject).

Why is it important?

As of August 1st, 2017

only **135** FEDERAL EMAIL DOMAINS out of **1315** HAD SOME FORM OF THE DMARC PROTOCOL DEPLOYED*

That's just 10%!

THE MAJORITY OF THESE AGENCIES **HAVE NOT ENABLED** THE FUNCTIONALITY

EXPOSING GOVERNMENT DATA AND **SYSTEMS TO HACKERS**

Who does it affect?

All US Federal Agencies

What are the key dates for meeting the mandate?

All US Federal Agencies have until **January 16th, 2018** to implement DMARC technology.

All US Federal Agencies have until **October 15th, 2018** to establish a policy using DMARC to reject all inbound unauthenticated messages.

*according to the non-profit Global Cyber Alliance leaving federal government data and systems exposed to hackers.

How can Forcepoint help agencies?

Forcepoint Email Security has the ability to check all inbound email for DMARC validation, and policies can be set to "allow", "quarantine" or "reject".

Visit **https://www.forcepoint.com/DMARC** for more information on how Forcepoint can help you meet the DMARC mandate or email **DMARC@forcepoint.com**

FORCEPOINT POWERED BY Raytheon

Protecting the human point.