AGARI

# FISMA Compliance for Anti-Phishing and Malware Defense

> *"Due to the preponderance of phishing attacks and their steadily increasing frequency and sophistication, anti-phishing and malware defense was added as a Cross-Agency Priority (CAP) goal beginning in FY15."*
>
> *— FY15 CIO Annual FISMA Metrics*

## WHAT ARE THE FISMA PERFORMANCE METRICS FOR ANTI-PHISHING AND MALWARE DEFENSE?

Specifically designed to reduce this risk, performance on Metrics 4.6 and 4.13 are measured on "percent (%) of incoming emails using email sending authentication protocols" and "percent (%) of sent email that is digitally signed" respectively.

If properly implemented using the DMARC standard, this can not only protect an agency from employee-to-employee inbound email spoofing but also can protect an organization's email infrastructure and definitively ensure its email domains cannot be hijacked by foreign nation-states or criminals in order to commit email phishing and malware attacks.

## WHAT IS DMARC?

- Domain-Based Message Authentication, Reporting and Conformance (DMARC) improves on earlier email authentication standards (SPF, DKIM, etc).
- Enables policies for email messages that fail authentication, including the option to block fraudulent emails so they are never delivered to intended targets.
- Includes domain-level data that not only identifies abuse, but also helps secure an organizations' infrastructure by providing visibility into legitimate email servers that the agency may not even be aware of.
- Provides detailed information about messages that pass or fail authentication, so organizations can take appropriate steps to improve their security, and authorities can take action against the perpetrators of email fraud.

## HOW DO I DEPLOY DMARC?

DMARC deployment is the most complete and effective means for outbound email authentication, but success is dependent on specialized email security skills and experience.  Most organizations find that the quickest and most efficient way to get up and running with DMARC is to work with partners like Agari who not can not only help to deploy DMARC but also provide critical value-added features.

## WHO IS AGARI?

Agari is a Silicon Valley Security-as-a-Service company.  We secure our customers' email domains and prevent them from being hijacked by criminals or unfriendly nation-states to commit phishing and malware attacks.  Agari is being leveraged today by several Federal agencies to solve this problem.

Agari's cloud-based solution aggregates data from 2.5 billion mailboxes, analyzing more than 8 billion messages per day, identifying more than 2 million malicious URLs per month, and blocking more than 200 million malicious emails per month. Founded by the thought leaders behind Cisco's IronPort solutions, Agari is a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security. Agari is headquartered in San Mateo, California.

## LEARN MORE

For more information, contact: **fedteam@agari.com** or download the DMARC Guide: **http://info.agari.com/agari-dmarc-primer.html**