AGARI

DHS Mandates DMARC for Email Security

December 2017 Progress Report

Executive Summary

On October 16, 2017, the U.S. Department of Homeland Security issued the Binding Operational Directive (BOD) 18-01 mandating the implementation of specific security standards to strengthen email and web site security. As part of this directive, specific federal agencies that operate .gov email domains must implement a DMARC monitoring policy (p=none) within 90 days. Furthermore, these agencies must move to a reject policy (p=reject) within one year.

As an update to the analysis performed by Agari in early November, we note the following:

Adoption increases to 47% — Between November 18, 2017, and December 18, 2017, 151 domains established a DMARC policy for the first time. This steady movement contributed to an overall DMARC policy rate of 47%. In itself, this is a significant improvement from just a month ago in November, when only 34% had a policy.

Strong early momentum for enforcement policies—There was also a 24% increase in the domains moving to a reject policy, the highest level of enforcement.

The agencies in aggregate are still unprotected – When the domains with no DMARC policy are added to those domains with a monitor-only policy, 84% of the domains are still unprotected from abuse.

Early adopters reaping benefits of DMARC enforcement – This month also validated the efforts of some early DMARC adherents by maintaining a low overall threat rate despite a massive increase in legitimate email campaigns.

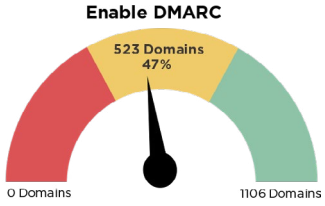
Government domains protected by Agari reached all-time highs – This month saw an unprecedented rate of protection for Agari government customers as a whole, with the sector achieving a 96% protection rate at the end of December.

This progress report summarizes the DMARC adoption trends and attainment levels for the federal email domains subject to the Directive.

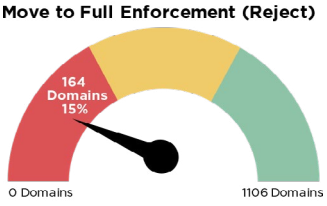
Some agencies at risk for not meeting key first DHS milestone – With less than three weeks until the first milestone requiring a DMARC policy of "p=none" or stronger, the clock is ticking. Based on the movement this past month, agencies without policies will need to increase the rate of adoption in order to meet the January 15, 2018, deadline.

[1] Includes all domains that send aggregate data to a 3rd party DMARC vendor.

DMARC Adoption Progress as of December 19, 2017

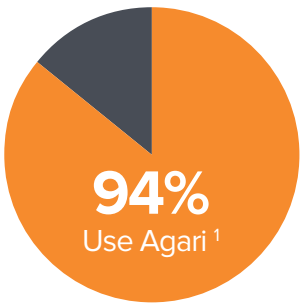


Adopt 'p=none' policy by 1/15/18



Adopt 'p=reject' policy by 10/16/18

Federal Domains* Using DMARC Implementation Services



DMARC Trends on Federal Agency Domains

Phishing continues to be a pervasive threat in the United States and around the world. The impact of these threats has been felt specifically by government agencies. Beyond the high-profile targeted attacks that have made headlines, criminals are executing phishing attacks leveraging the brand name of agencies. From month to month, Agari continues to see spoofing attacks against our federal customers. As the following chart indicates, on the email-sending and defensive domains that we monitor, 8% of total email volume was malicious or failing authentication. Almost 90% of our federal domains were targeted by domain abuse, a ratio that was virtually unchanged since the previous month.

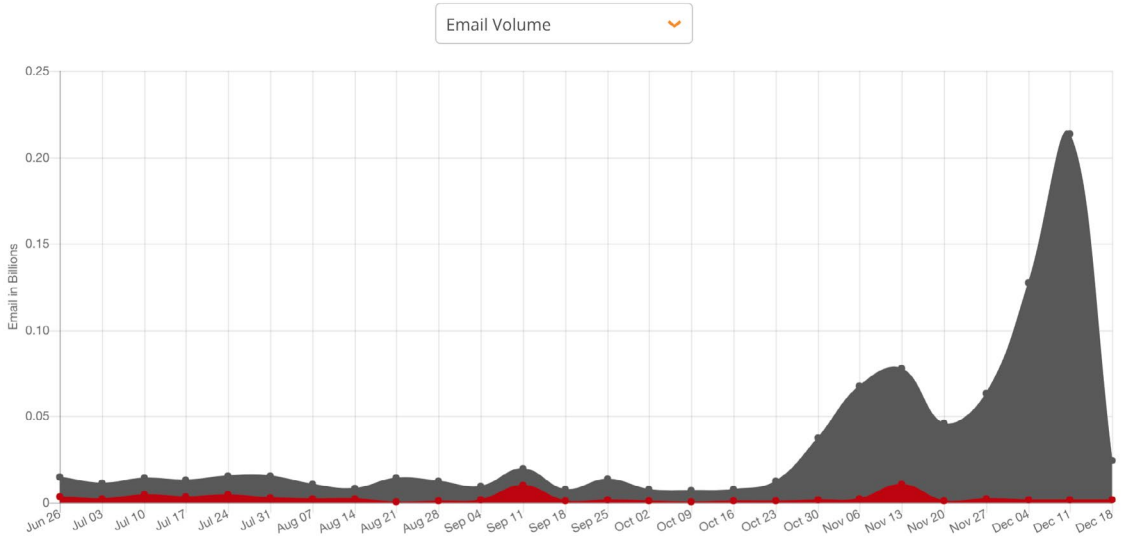
Agari Email Trust Network

DMARC Report Data on Government Domains: 6 Months Ending December 26, 2017

Agari Protected	Threat Volume	Threat Rate
871.62M Total Emails	68.79 M Malicious Emails	7.89% Malicious Emails
473 Total Domains	406 Domain Targeted	85.84% Domain Targeted

Another notable trend was the sheer uptick in government email traffic around the time of the Directive. The chart below depicts the exponential rise in email from key government customers.

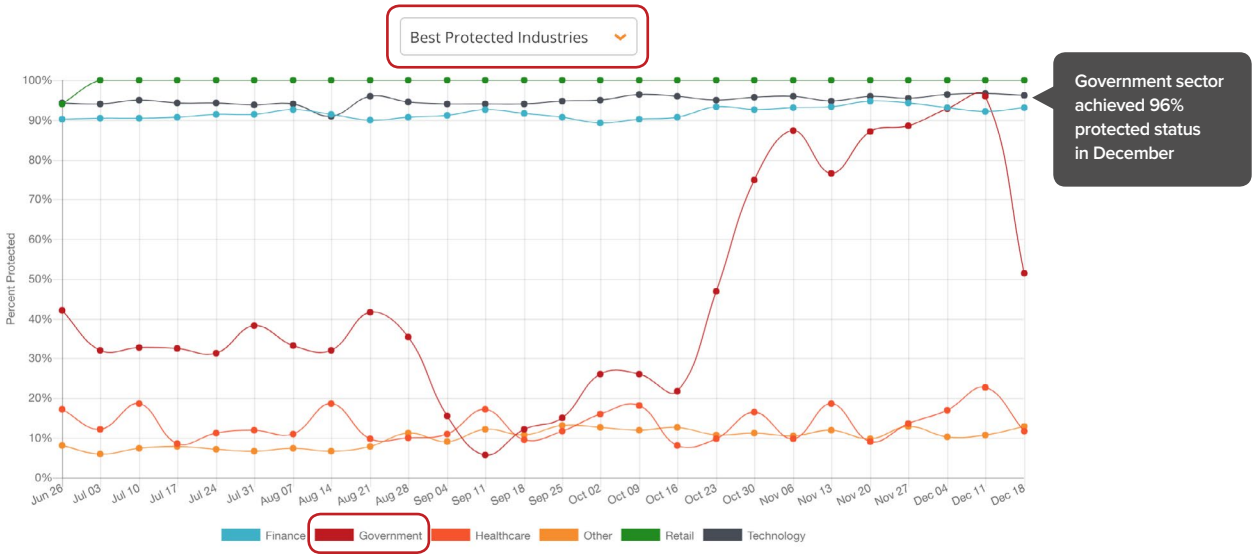
Threat Trends Over Time



For more DMARC insights and trends, visit www.agari.com/email-threat-center/

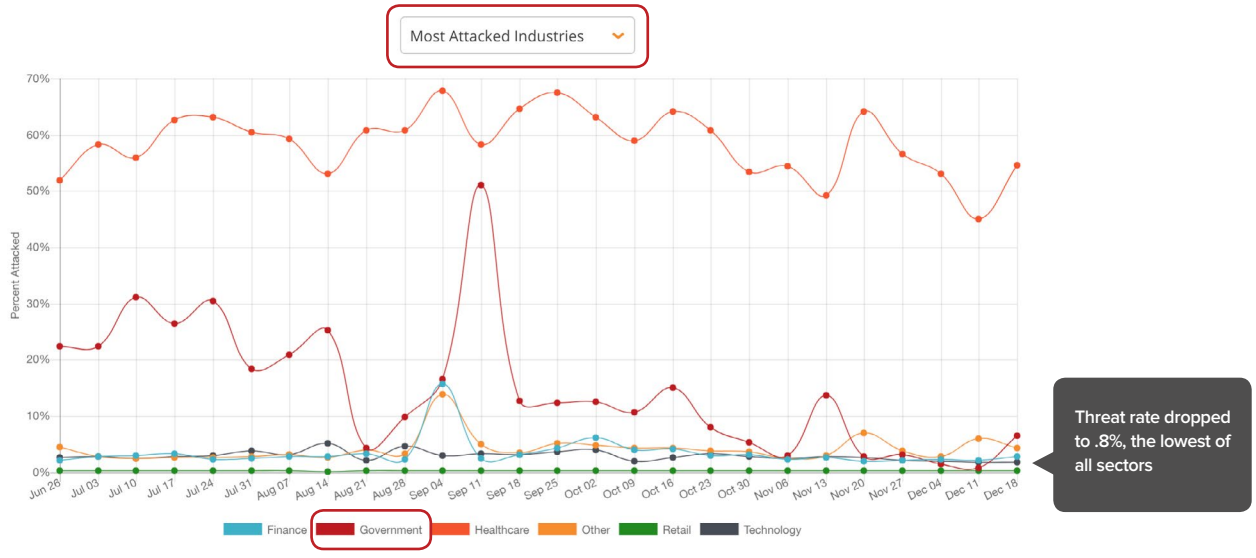
Switching to the view of protected domains, the same overall period marked another milestone. Over the last month and a half, the protection ratio (measured domains with a reject or quarantine policy) for government domains visible to the Threat Center soared from 22% to 96%. For the first time since Agari has been tracking and ranking customer sectors by their authentication status, the government sector surpassed 90% of its domains protected with an enforcement policy. In fact, towards the end the measurement period, the government sector was riding the heels of the Retail and Technology sectors, the perennial authentication champs as determined by the Agari Email Threat Center.

Protection Status for Government Domains Tracked by Agari Threat Center



Finally, as a measure of the benefits of strong enforcement of unauthenticated email traffic, the overall threat rate for government customers dipped well below 1%.

Attack Rate Status for Government Domains Tracked by Agari Threat Center

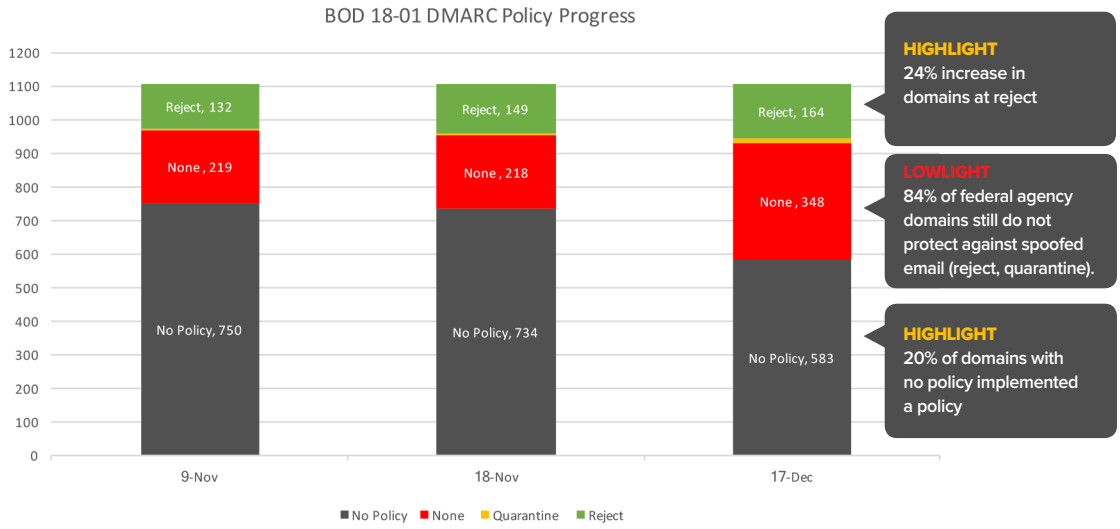


For more DMARC insights and trends, visit www.agari.com/email-threat-center/

DMARC Adoption Rates: Performance Against the Mandate

The following chart depicts the month over month progress of the 1,106 US government domains subject to the DHS directive. While there has been positive movement since Agari's initial analysis in November, DMARC adoption for the US government overall continues to be very low, enabling malicious actors to abuse that trust and leaving agencies at risk of missing the milestones prescribed in the Directive.

Meeting the Mandate: Highlights and Lowlights



DMARC Adoption – Over the course of the month, 151 additional domains established a DMARC policy. Last month, 66% of the domains had no policy; the positive movement in core policy creation dropped that unwanted distinction down to 53%. While still low, the set of government domains now has a significantly better adoption level than the commercial sector, where two-thirds (67 percent) of the domains have not published any DMARC policy.

None (Monitor) Policy – As of December 17, almost a third (31%) of in-scope federal domains have a Monitor policy. The "p=none" policy is the minimal level that that federal agencies need to implement by the 90 day deadline, which is January 15, 2018. This policy represents the start of the DMARC journey, allowing domain owners to monitor for authentication abuse, but not prevent it. While an important first step, by definition it still leaves agencies unprotected. When combined with the number of domains with no DMARC policy whatsoever, close to 84% of in-scope federal agency domains are vulnerable to digital deception, leaving their constituents and email recipients exposed to phishing and fraud. Taken together, the end result is just a marginal improvement over the last month, where the sum of domains with no DMARC policy and those with a monitor only policy was 952 (86%).

Quarantine Policy – Less than 1% (only 5 domains) were at the initial level of enforcement, or a Quarantine policy (which sends messages that fail DMARC tests into the spam folder). This policy attainment represented just half of a percentage point improvement over the previous month.

Reject Policy – The delta between the all-important reject policy from November and December was +20%. Over the course of the month, 15% (164 domains) implemented a Reject policy to block messages that fail authentication. Of these domains at a Reject policy, almost 68% of them were so-called defensive domains, which do not send mail. As per the DHS mandates, all the relevant government agency domains need to be at Reject policy within one year (October 16, 2018).

[1] For more details on DMARC adoption statistics for the Fortune 500, Financial Times Stock Exchange 100, and Australian Securities Exchange, see the Agari report Open Season for Phishers at agari.com/dmarcreportus/

A Bright Spot for DMARC Deployment

A particular bright spot for federal DMARC deployment is that 23 agencies have achieved 100 percent deployment. Additionally, many larger agencies have deployed DMARC across numerous domains, or have nearly completed adoption. The Department of Health and Human Services is the only federal agency to have deployed DMARC across more than 100 domains.

Agency Name	DMARC Deployments	Domains Managed	Percentage Adoption
Administrative Conference of the United States	1	1	100
Consumer Product Safety Commission	10	10	100
Corporation for National & Community Service	13	15	86.6
Defense Nuclear Facilities Safety Board	1	1	100
Department of Education	11	15	73.3
Department of Health And Human Services	107	121	88.4
Department of the Interior	71	72	98.6
Department of the Treasury	81	99	81.8
Department of Veterans Affairs	3	3	100
Equal Employment Opportunity Commission	1	1	100
Export/Import Bank of the U.S.	1	1	100
Federal Communications Commission	8	8	100
Federal Elections Commission	1	1	100
Federal Labor Relations Authority	1	1	100
Federal Retirement Thrift Investment Board	5	5	100
Federal Trade Commission	23	23	100
General Services Administration	84	114	73.6
Millennium Challenge Corporation	2	2	100
National Aeronautics and Space Administration	4	4	100
National Labor Relations Board	1	1	100
National Science Foundation	5	6	83.3
National Transportation Safety Board	1	1	100
Nuclear Regulatory Commission	2	2	100
Occupational Safety & Health Review Commission	1	1	100
Pension Benefit Guaranty Corporation	1	1	100
Social Security Administration	2	2	100
Surface Transportation Board (STB)	1	1	100
Terrorist Screening Center	1	1	100
U. S. Holocaust Memorial Museum	1	1	100
U. S. International Trade Commission	1	1	100

Case Study: The DMARC Journey for US Health and Human Services

Health and Human Services (HHS) manages 120 top-level domains, including the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), the Centes for Medicare and Medicaid Services (CMS) and Healthcare.gov. HHS sends as many as 30 million emails per day during flu season and open enrollment and uses nine different email service providers. The following information is summarized from a webinar presented by the HHS.

In 2015, HHS noticed a significant increase in threats against healthcare. The agency implemented SPF, but it wasn't delivering the needed outcome. HHS recognized the opportunity to prevent threats targeting its domains with DMARC because it had been widely implemented in finance.

In 2016, HHS began evaluating DMARC on healthcare.gov. Ultimately, HHS partnered with Agari to aggregate the data from the reports to provide the information they needed. During its pilot program, HHS identified threats against its domains that they could have stopped if DMARC had been implemented. During open enrollment in 2016, CMS deployed DMARC in one month – Healthcare.gov was ready for it. And for the first time, there were no phishing campaigns against Healthcare.gov.

As HHS continued its widespread deployment, it followed a pattern of preparing and reporting, monitoring and assessing, and operating and securing. HHS began by deploying DMARC and SPF on every domain that doesn't send email. Next, HHS worked with third-party service providers, such as GovDelivery, to deploy DMARC, SPF and DKIM to protect the majority of its outreach mail. With 27 active domains protected by DMARC, HHS is protecting 94% of outbound messages.

As an additional benefit, HHS has been able to leverage its portal with multiple communities to trim down activity in the wild. Threat feeds have enabled DHS cybersecurity teams to identify threats for domain takedowns. Operations have been improved with better visibility to manage mail servers. Finally, HHS is able to easily identify its third-party service providers, presenting contractual opportunities for cost saving.

Conclusion

Clearly, some agencies are aware of the threat of digital deception and have taken appropriate countermeasures. A few federal agencies, including the US Department of Health and Human Services, have taken the initiative by enabling DMARC. Moreover, they have configured it in the most strict "reject" mode so that email service providers can automatically reject phishing emails impersonating their agency. However, among other early adopters, a significant number of their deployments are "p=none," which does nothing to prevent these attacks. DMARC adoption is of little use unless organizations move to a Quarantine or Reject policy.

The analysis in this paper has shown that while federal agencies are making progress in the wake of the specific timelines set forth in BOD 18-01, most remain unprotected against phishing. Almost 53% of federal agencies' domains currently do not have a DMARC policy. For those that do, the majority still maintain a monitor-only "p=none" policy that doesn't protect their constituents. These agencies and their email recipients remain vulnerable to domain spoofing and phishing attacks.

Deploying a DMARC policy where p=none is simple, but it is only the first step. To fully protect against phishing threats against both the federal government and the public at large (and maintain strong email governance), federal agencies must ultimately move to Quarantine and Reject policies.

To learn more about DMARC and how to comply with BOD 18-01, visit
agari.com/dmarc-security-for-government-agencies/

About DMARC

Digital deception emails trick users into clicking on hyperlinks leading to websites that steal their passwords, install ransomware or con unsuspecting victims into sending money. This type of fraud represents billions of dollars in losses per year and is completely preventable if organizations adopt an open standard called DMARC (Domain-based Message Authentication, Reporting & Conformance).

According to DMARC.org, DMARC is designed to:

- Minimize false positives.
- Provide robust authentication reporting.
- Assert sender policy at receivers.
- Reduce successful phishing delivery.
- Work at Internet scale.
- Minimize complexity.

Aside from the DHS mandate issued in October, the DMARC standard has been previously cited as a key control to help agencies reduce the likelihood that their domains and brand will be used in an attack. These recommendations came from government bodies including:

- **FISMA:** DMARC (and email authentication) is evolving into a key metric that impacts the FISMA scorecard against an agency.
- **NIST:** NIST recommends using DMARC authentication tools to provide protection against phishing (SP 800-177, Trustworthy Email, Section 4.6).
- **FTC:** The FTC recommends wider implementation of DMARC to combat phishing attacks (Staff Perspective, March 2017).

How DMARC Works

DMARC is designed to be deployed in stages. When an agency implements DMARC, there are three levels of policies that can be applied to their domains:

Monitor (None) – With this initial policy, unauthenticated messages are monitored, but still delivered to the inbox. This configuration provides feedback about servers using the domain name in the "From:" header of the email messages they send. The domain owner uses this information to make adjustments to their SPF and DKIM configurations until all of their legitimate mail sources are properly authenticated. The DHS directive mandates a policy of "none" as a minimum by the 90 day deadline.

Quarantine – When all an agency's legitimate mail sources are properly authenticated, the DMARC policy can be tightened to "p=quarantine", which sends unauthenticated messages to the recipient's spam folder.

Reject – A reject policy is the strictest configuration, in which unauthenticated messages are blocked outright.

DMARC must also be deployed on the receiver side, by email service providers. Currently, the major email service providers—Microsoft, AOL, Google and Yahoo!—have deployed DMARC, but smaller email service providers or a self-hosted email server may not provide the same level of protection.

For more information on the DMARC standard, see
www.agari.com/dmarc-guide/

About Agari

Agari, a leading cybersecurity company, is trusted by leading Fortune 1000 companies to protect their enterprise, partners and customers from advanced email phishing attacks. The Agari Email Trust Platform is the industry's only solution that 'understands' the true sender of emails, leveraging the company's proprietary, global email telemetry network and patent-pending, predictive Agari Trust Analytics to identify and stop phishing attacks. The platform powers Agari Enterprise Protect, which help organizations protect themselves from advanced spear phishing attacks, and Agari Customer Protect, which protects consumers from email attacks that spoof enterprise brands. Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is backed by Alloy Ventures, Battery Ventures, First Round Capital, Greylock Partners, Norwest Venture Partners and Scale Venture Partners. Learn more at http://www.agari.com and follow us on Twitter @AgariInc.