FORTRA

GUIDE (Agari)

DHS Mandates DMARC for Email Security

July 2018 BOD 18-01 Progress Report

Executive Summary

On October 16, 2017, the U.S. Department of Homeland Security (DHS) issued its Binding Operational Directive (BOD) 18-01, which mandates the implementation of specific security standards to improve email and web site security. As part of this directive, executive branch agencies that operate gov email domains are required to implement a DMARC reject policy *("p=reject")* by **October 16, 2018** Domain-based Message Authentication, Reporting and Conformance (DMARC) is a powerful email authentication, policy, and reporting protocol that prevents domain spoofing by malicious actors.

Agari has been working closely with the US. Department of Homeland Security since last year to monitor and report on federal government DMARC adoption. This report examines executive branch DMARC adoption as of July 15, 2018.

Executive branch DMARC adoption increases to 81%

As of July 15, 2018, executive branch DMARC adoption has increased to 81%. This includes the basic monitoring policy, *"p-none,"* the intermediate containment policy. *"p-quarantine,"* and the ultimately required blocking policy, *"p=reject."*

More than half of executive branch domains have reached "p-reject" ahead of deadline

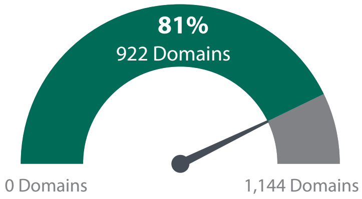
As of July 15, 2018 (three months ahead of deadline), 52% of the 1,144 executive branch domains subject to BOD 18-01 have implemented DMARC at its strongest enforcement level "*p=reject*".

Defensive domains comprise the majority of domains brought to enforcement

As of July 15, 2018, 66% of the domains that have a *"p-reject"* policy are domains configured not to send email, also known as defensive domains. Moving ***defensive domains*** to a DMARC enforcement policy is generally an easier process than moving active domains that send email, and also need to account for 3 parties sending email on the agency's behalf as well as specific mail servers permitted to send email

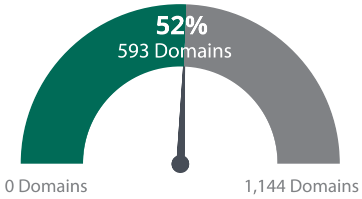
PROGRESS TO DATE

Enable DMARC



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

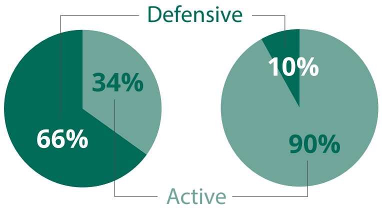
Move to Full Enforcement
"p=reject"



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

Domains at *"p=reject"*

Domains Out of Compliance



DMARC Adoption Rates: Performance Against the Mandate

The chart on the right depicts DMARC adoption of the 1,144 executive branch domains subject to the DHS directive. These adoption rates suggest that the BOD mandate has been a positive Initiative for the US government, as more than half of all executive branch domains are now protected from malicious actors that would seek to abuse trusted government communication

DMARC Adoption

DMARC adoption within the executive branch has steadily climbed since January 2018. As of July 15, 2018 only one fifth (19%) of executive branch domains had no policy. This is significantly better adoption than the commercial sector, where two-thirds (67%) of the Fortune 500 have not published any DMARC policy

None (Monitor) Policy

As of July 15, 2018 one quarter (26%) of executive branch domains have adopted a monitor policy. The "p-none" policy was the minimal level required for implementation ahead of BOD 18-01's original 90-day deadline, which was January 15, 2018. The "p=none" policy enables domain owners to monitor their email for authentication issues, but does not prevent them. This policy is an important first step for DMARC adoption, but still leaves agencies unprotected. When combined with the 19% of executive domains that have no DMARC policy, almost half of executive branch domains are still vulnerable to domain spoofing, leaving their email unprotected from phishing, fraud and identity deception attacks

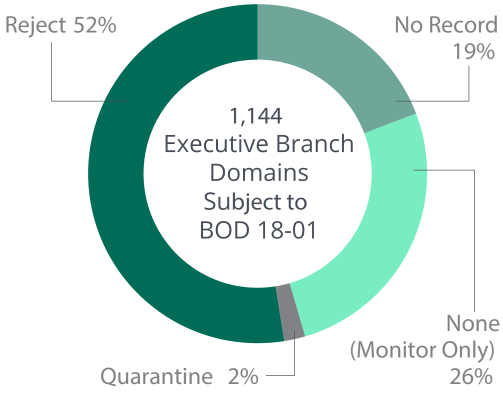
Quarantine Policy

Only 26 executive branch domains (two percent) have implemented a quarantine policy, which sends messages that fail DMARC authentication into the spam folder. As a bit of interesting trivia, 14 of those domains are managed by the DHS

Reject Policy

Ultimately, BOD 18-01 requires all executive branch domains to be secured with a "p-reject" DMARC policy by October 16, 2018. A reject policy blocks messages that fall DMARC authentication from being delivered. As of July 15, 2018, more than half (52%) of executive branch domains have adopted a reject policy

U.S. FEDERAL DMARC
ADOPTION & PROGRESS



Defensive Domains in BOD 18-01

A significant pattern observed during this upolate concerns the proportion of defensive domains or otherwise non email-sending domains related to the total number of domains in scope for BOD 18-01. In contrast with active domains that are permitted to send email, defensive domains have a specific SPF configuration that indicates they will never send email. For this set of domains, the DMARC configuration process is often streamlined because there is no need to manage and align 3rd party senders and perform other safeguards to prevent receivers from deleting legitimate mail that fails DMARC authentication, Based on Agari's analysis, of the 593 domains that are currently at "p-reject" policy, 393 (6696) are defensive domains that do not send email. Turning to the domains that are currently not in compliance for the upcoming deadline-specifically the 526 domains that currently do not have a DMARC record or are at a "p=none policy-only 10 percent of those domains can be characterized as defensive. This would suggest that bringing the remaining half of domains to compliance could involve more work on the part of the agencies involved.*

Making the Grade: Passing Marks for DMARC Deployment

Ahead of the October 16, 2018 deadline for BOD 18-01, 28 executive branch agencies have already protected all of their domains with "p-reject " Additionally, many larger agencies have made great progress toward full adoption and implementation of "p-reject" The Department of Health & Human Services has secured 97 domains at "p-reject"- the most of any agency.

Executive Branch Agency DMARC Deployment-as of July 15, 2018

AGENCY NAME	DOMAINS	DMARC DEPLOYMENTS (ANY POLICY)	DMARC DEPLOYMENTS ("P=REJECT")
Consumer Financial Protection Bureau	10	10 (100%)	1 (10%)
Consumer Product Safety Commission	10	10 (100%)	10 (100%)
Corporation for National & Community Service	14	13 (93%)	0 (0%)
Court Services and Offender Supervisio	4	4 (100%)	4 (100%)
Defense Nuclear Facilities Safety Board	1	1 (100%)	1 (100%)
Department of Education	14	10 (71%)	6 (43%)
Department of Health & Human Services	118	113 (96%)	92 (78%)
Department of Homeland Security	31	25 (81%)	6 (19%)
Department of Housing & Urban Development	11	10 (91%)	8 (73%)
Department of Justice	75	68 (91%)	65 (87%)
Department of Labor	21	18 (86%)	17 (81%)
Department of State	19	19 (100%)	9 (47%)
Department of the Interior	70	66 (94%)	41 (59%)
Department of the Treasury	97	94 (97%)	54 (56%)
Department of Transportation	26	26 (100%)	17 (65%)
Department of Veterans Affair	3	3 (100%)	3 (100%)
Environmental Protection Agency	15	14 (93%)	8 (53%)
Executive Office of the Preside	25	15 (60%)	11 (44%)
Export/Import Bank of the U.S.	1	1 (100%)	1 (100%)
Federal Communications Commission	8	8 (100%)	8 (100%)
Federal Deposit Insurance Corporation	7	7 (100%)	7 (100%)
Federal Housing Finance Agency	2	2 (100%)	2 (100%)
Federal Maritime Commission	1	1 (100%)	1 (100%)
Federal Reserve Board of Governors	12	11 (92%)	9 (75%)
Federal Retirement Thrift Investment Board	5	5 (100%)	5 (100%)
Federal Trade Commission	23	23 (100%)	23 (100%)
General Services Administration	100	95 (95%)	57 (57%)
Institute of Museum and Library Services	1	1 (100%)	1 (100%)

AGENCY NAME	DOMAINS	DMARC DEPLOYMENTS (ANY POLICY)	DMARC DEPLOYMENTS (“P=REJECT”)
Millennium Challenge Corporation	2	2 (100%)	2 (100%)
Morris K. Udall and Stewart L. Udall Foundation	2	2 (100%)	2 (100%)
National Archives & Records Administration	22	20 (91%)	19 (86%)
National Endowment for the Arts	2	2 (100%)	2 (100%)
National Gallery of Art	1	1 (100%)	1 (100%)
Nuclear Regulatory Commission	2	2 (100%)	2 (100%)
Occupational Safety & Health Review Commission	1	1 (100%)	1 (100%)
Office of Government Ethi	2	2 (100%)	2 (100%)
Office of Personnel Manageme	23	17 (74%)	10 (43%)
Securities & Exchange Commission	2	2 (100%)	2 (100%)
Social Security Administration	4	3 (75%)	3 (75%)
Terrorist Screening Center	1	1 (100%)	1 (100%)
U.S. Commission on International Religious Freedom	1	1 (100%)	1 (100%)
U.S. Department of Agriculture	42	39 (93%)	29 (69%)
U.S. Office of Special Couns	2	2 (100%)	2 (100%)
U.S. AbilityOne	2	2 (100%)	2 (100%)
U.S. Access Board	1	1 (100%)	1 (100%)
U.S. African Development Foundation	2	2 (100%)	2 (100%)
U.S. Holocaust Memorial Museum	1	1 (100%)	1 (100%)
U.S. Postal Service	9	9 (100%)	9 (100%)

Conclusion

With less than three months until the final BOD 18-01 deadline, the U.S. Government has made tremendous strides forward in its DMARC adoption and compliance efforts. Most federal agencies and the citizens they serve are now realizing the benefits of DMARC. Executive branch agencies such as the Department of Health and Human Services have implemented a "p=reject" policy across hundreds of domains to automatically block phishing email attacks and prevent domain spoofing. Yet hundreds of other federal domains still remain vulnerable to these attacks.

If the January 2018 deadline proved that deploying a "p=none" DMARC policy is simple, then the past six months have proven that it is possible to reach the final step of "p=reject" ahead of the October deadline with help from service providers like Agari. To fully reach compliance with BOD 18-01, and to protect the federal government from phishing attacks, many more executive branch agencies must still implement "p=reject "B "But in comparison to the private sector, the US. Government should serve as a shining example for the implementation of common security standards.

For more Agari resources on BOD 18-01: agari.com/bod-18-01/