Agency Plan of Action for BOD 18-01

Prepared by	Click here to enter text.
On behalf of (Federal agency)	Click here to enter text.
Date	

Contents

Introduction

On Monday 16th October 2017, the Department of Homeland Security (DHS) published Binding Operational Directive 18-01. The BOD requires civilian agencies to meet the following objectives in order to “Enhance Email and Web Security” (deadlines are listed in chronological order and are expressed relative to the date of publication of the BOD):

BOD Ref.	Requirement	Deadline
1.	Submit “Agency Plan of Action for BOD 18-01” to DHS	30 days
2.	Send monthly project status reports to DHS	From 60 days
3.1.	Deploy STARTTLS on all internet-facing mail servers	90 days
3.2.	Deploy valid SPF record for all second-level domains	90 days
3.3.	Deploy valid DMARC record for all second-level domains (with at least a “monitor” or “p=none” policy)	90 days
4.1.	Disable SSLv1 & v2 on mail servers	120 days
4.2.	Disable 3DES & RC4 ciphers on mail servers	120 days
5.1.	Enable HTTPS (with HSTS) for all publicly accessible websites & web services	120 days
5.2.	Disable SSLv1 & v2 on web servers	120 days
5.3.	Disable 3DES & RC4 ciphers on web servers	120 days
5.4.	Provide DHS with list of second-level domains that can be HSTS preloaded (thereby enforcing HTTPS for all associated subdomains)	120 days
6.	Add NCCIC to DMARC record as recipient of aggregate reports	15 days from when NCCIC is ready
7.	Deploy “p=reject” DMARC policy for all second-level domains	1 year

This response is submitted to frame the agency’s overarching plan to comply with the requirements of BOD 18-01 and specifically to meet the initial 30-day deadline (BOD Ref. 1 above).

Assumptions, dependencies, constraints and unknowns

1. The list of second-level domains for which the agency is responsible and for which it will assume responsibility for BOD 18-01 compliance is included in the Appendix.

2. The hierarchical nature of DMARC means that the agency may discover subdomains relating to its second-level domains that introduce dependencies that may in turn add complexity and effort to the implementation plan.

3. Until the agency has a better understanding of the complexity of its email ecosystem and what DMARC deployment entails, it will be difficult to know whether help from third parties and vendors will be required. In the event that such services are required, additional time and effort may need to be spent in sourcing such assistance.

4. The DHS BOD 18-01 refers to SPF and DMARC, but does not cover DKIM. DKIM is however a requirement for deploying DMARC. Many legacy gateways do not support DKIM signing, where these are identified the agency will need to introduce new infrastructure which possesses the requisite abilities.

5. DNS must support SPF, DMARC and DKIM records – the latter can be large, and may need multiple records to be concatenated. Not all DNS platforms support this – therefore this should be established early on in case a DNS migration is required as part of the overall project.

6. Some third parties choose to authenticate in a way that contradicts the requirements of DMARC and therefore cannot pass the alignment check mandated by DMARC. These third parties must be identified early in the project, and a mitigation/migration strategy established. A vendor is particularly useful in this situation as they will understand what a third party can or cannot do, rather than what they say they can or cannot do.

Agency’s compliance plan

Each of the atomic requirements of BOD 18-01 are laid out below with the agency’s corresponding plan to comply within the given timeframe. All deadlines are expressed relative to date of publication of the BOD unless otherwise stated with associated plans and risk assessments.

1. Submit “Agency Plan of Action for BOD 18-01” to DHS

DHS requirement	Within 30 calendar days after issuance of this directive, develop and provide to DHS an “Agency Plan of Action for BOD 18-01”
Deadline	30 days (November 15, 2017)
Status	Completed
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

2. Send monthly project status reports to DHS

DHS requirement	Provide a report to DHS on the status of that implementation. Continue to report every 30 calendar days thereafter until implementation of the agency’s BOD 18-01 plan is complete.
Deadline	Monthly from 60 days (December 15, 2017)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

3.1. Deploy STARTTLS on all internet-facing mail servers

DHS requirement	Configure all internet-facing mail servers to offer STARTTLS
Deadline	90 days (January 14, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

3.2. Deploy valid SPF record for all second-level domains

DHS requirement	All second-level agency domains to have valid SPF records
Deadline	90 days (January 14, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

3.3. Deploy valid DMARC record for all second-level domains

DHS requirement	All second-level agency domains to have valid DMARC records, with at minimum a DMARC policy of “p=none” and at least one address defined as a recipient of aggregate and/or failure reports.
Deadline	90 days (January 14, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

4.1. Disable SSLv1 & v2 on mail servers

DHS requirement	Ensure Secure Sockets Layer (SSL)v2 and SSLv3 are disabled on mail servers.
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

4.2. Disable 3DES & RC4 ciphers on mail servers

DHS requirement	Ensure 3DES and RC4 ciphers are disabled on mail servers.
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

5.1. Enable HTTPS (with HSTS) for all publicly accessible websites & web services

DHS requirement	Ensure all publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS).
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

5.2. Disable SSLv1 & v2 on web servers

DHS requirement	Ensure SSLv2 and SSLv3 are disabled on web servers.
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

5.3. Disable 3DES & RC4 ciphers on web servers

DHS requirement	Ensure 3DES and RC4 ciphers are disabled on web servers.
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

5.4. Provide DHS with list of second-level domains that can be HSTS preloaded

DHS requirement	Identify and provide a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.
Deadline	120 days (February 13, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

6. Add NCCIC to DMARC record as recipient of aggregate reports

DHS requirement	Add the National Cybersecurity & Communications Integration Center (NCCIC) as a recipient of DMARC aggregate reports.
Deadline	Within 15 days of the establishment of NCCIC centralized reporting location
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

7. Deploy “p=reject” DMARC policy for all second-level domains

DHS requirement	Set a DMARC policy of “reject” for all second-level domains and mail-sending hosts.
Deadline	1 year (October 16, 2018)
Status	Choose an item.
Plan	Click here to enter text.
Risk	Choose an item.
Risk detail	Click here to enter text.
Risk mitigation	Click here to enter text.
DHS comments	Click here to enter text.

On-going project management

It is intended that the format laid out above will form the basis of the on-going monthly reporting framework that the agency will use in order to report to the DHS on the status of implementation. The agency will therefore provide the agency with an on-going consolidated summary of the following for each of the requirements:

1. Status
2. Plan
3. Risk
4. Risk detail
5. Risk mitigation

Appendix: list of agency domains

Domain	Authoritative DNS host	Notes	SPF	DMARC
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐
Click here to enter text.	Click here to enter text.	Click here to enter text.	☐	☐