FORTRA

GUIDE *(Agari)*

A Federal Agency Guide to Complying with Binding Operational Directive (BOD) 18-01

Table of Contents

Introduction

The purpose of this document is to provide tactical guidelines to assist Federal agencies in complying with the Department of Homeland Security Binding Operational Directive (BOD) 18-01 requirements.

For organizations looking for assistance in developing a Plan of Action for BOD 18-01 or in executing an existing plan, contact us at https://www.agari.com/federal-dmarc-consultation.

Required Actions Overview

The Department of Homeland Security issued a binding directive on October 16, 2017, ordering all Federal agencies to enhance their email and web security programs. The directive references several milestones that agencies must meet in order to show progress and ultimately compliance with the directive. The following outlines these requirements and associated deadline from the issue date of October 16, 2017.

Ref. #	Required Action	Deadline (Date)
1.	Submit to DHS - Agency Plan of Action for BOD 18-01	11/15/17
Email Security		
2.	All Internet-facing mail servers to offer STARTTLS	01/14/18
3.	All second-level agency domains to have valid SPF/DMARC records, with minimum DMARC policy of "p=none" & at least one defined recipient of aggregate and/or failure DMARC reports	01/14/18
4.	Secure Sockets Layer (SSL) v2 and SSL v3 are disabled for mail servers	02/13/18
5.	3DES and RC4 ciphers are disabled on mail servers	02/13/18
6.	National Cybersecurity & Communications Integrations Center (NCCIC) added as a recipient of aggregate reports	15 days from creation of NCCIC
7.	Set DMARC policy of "p=reject" for all second-level domains and mail-sending hosts.	10/16/18
Web Security		
8.	All publicly accessible Federal websites & web services provide services through a secure connection (HTTPS-only with HSTS)	02/13/18
9.	Secure Sockets Layer (SSL) v2 and SSL v3 are disabled on web servers	02/13/18
10.	3DES and RC4 ciphers are disabled on webservers	02/13/18
11.	Identify and provide a list of agency second-level domains that can be HSTS preloaded for which HTTPS will be enforced for all subdomains, to DHS	02/13/18
Status of Implementation		
12.	Submit to DHS - Report on the status of the BOD 18-01 Implementation	12/15/17
12.3	Submit to DHS – Subsequent reports on the status of the BOD 18-01 Implementation until completion	Every 30 days from 12/15/17

Required Actions – Email Security

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

In order to meet this required action, agencies should:

1.1. Create a document which describes the Agency's plan and milestones along with any associated risks, dependencies, or constraints that will be completed to comply with the directive. Agari has provided a template that agencies can use to help complete this action: Agari_BOD_1801_Plan_of_Action_TEMPLATE.xlsx.

1.2. Email the "Agency Plan of Action" to FNR.BOD@hq.dhs.gov by November 15, 2017.

1.3. Upon submission of the Agency Plan of Action for BOD 18-01, the agency must begin implementation immediately.

2. All Internet-facing mail servers to offer STARTTLS

STARTTLS is used to upgrade an existing insecure SMTP connection to a secure one using SSL/TLS. STARTTLS is intended to protect against attackers using passive monitoring techniques (e.g. passive man-in-the-middle attacks). In order to meet this required action, agencies should:

2.1. Identify all Internet-facing mail servers receiving or sending email on the behalf of the agency.

2.2. Modify the mail server configuration file to enable STARTTLS.

Please note that configuring a mail server to offer STARTTLS will vary from system to system. We recommend you refer to your mail server's documentation for explicit instructions on enabling STARTTLS and its associated options. In most cases, a typical configuration may include the following:

2.2.1. Generate, activate, and import a TLS client certificate into the mail server.

2.2.2. For receiving email - configure the mail server to accept a TLS connection, require existence of a TLS certificate, and require certificate validation.

2.2.3. For sending email - configure the mail server to attempt a TLS connection ondelivery, and optionally offer a TLS client certificate.

2.2.4. Verify that the mail server is correctly configured to offer STARTTLS.

3. All second-level agency domains to have valid SPF/DMARC records, with minimum DMARC policy of "p=none" & at least one defined recipient of aggregate and/or failure DMARC reports

In order to meet the required action, agencies should complete the following:

3.1. Catalog all domains registered or belonging to the agency and categorize the domain on whether or not valid email is sent on its behalf.

3.2. For each domain create a valid DMARC record:

3.2.1. Create a valid recipient to receive aggregate and/or failure DMARC reports.

3.2.2. Create a DMARC record using a tool such as one provided by Agari at: https://www.agari.com/resources/tools/dmarc

3.2.2.1. Enter the agency domain that you intend to create a DMARC record for and click 'Submit'.

3.2.2.2. Click 'Create DMARC Record' to begin creating your record.

3.2.2.3. Under the option 'How strict do you want your DMARC policy to be?' select 'Monitor only' in the drop-down.

Selecting *'Monitor only' will meet the BOD 18-01 directive for minimum DMARC policy of "p=none".*

3.2.2.4. Under the option 'Where do you want Aggregate Reports to be sent?',

Agari is listed as a recipient and can help to automatically identify, track, and manage internal and 3rd party senders.

If you would like assistance with analyzing your DMARC reports enter the recommended Agari email address. However, you may optionally add your recipient email address created in item 3.2.1.

Entering an email address within this section meets the BOD 18-01 directive for including at least one valid email address to receive DMARC reports.

3.2.2.5. Enter all other required details and click 'Next'.

3.2.2.6. Click 'Show Instructions' to view instructions on how to publish the record. You will need to work with your DNS server administrator to publish your DMARC record.

If an existing record exists, verify that the record meets the BOD 18-01 requirements for this required task. If so, the existing record can be used.

3.2.2.7. For newly published DMARC records, verify that the DMARC record is successfully published. The Agari DMARC look-up tool can be used to verify that the DMARC record is published: https://www.agari.com/resources/tools/dmarc/

3.2.3. If you have added your own agency email address to receive DMARC reports, verify that the reports are being received internally.

3.3. For each domain create a valid SPF record:

3.3.1. Prior to creating an SPF record, we recommend reviewing your aggregate DMARC reports or work with Agari to assist in interpreting your reports. DMARC reports are extremely valuable in determining which IP addresses are sending email on your behalf, and/or domains that are being used or abused.

3.3.2. For sending domains, identify all valid IP addresses sending email and include those in the SPF record. At a basic, the SPF record should look like the following:

v=spf1 ip4:x.x.x.x ~all
where v = version tag
ip4:x.x.x.x = valid IP addresses that are authorized to send mail (list all that apply)
~all = soft SPF fail (multiple IP addresses can be added)

3.3.3. For sending domains where an authorized 3rd party sender is configured to send on the agency's behalf, an 'include' attribute should be added to the SPF record. The 'include' attribute should be recorded similar to the following:

v=spf1 ip4:x.x.x.x include:_spf.3rdpartyexample.com ~all
where v = version tag ip4:x.x.x.x = valid internal IP address that are authorized to send mail include:_spf.3rdpartyexample.com = valid reference to authorized IP's or domains of the authorized 3rd party (multiple include attributes can be added)
~all = soft SPF fail

3.3.4. For non-sending domains, the SPF record should look like the following:

v=spf1 –all
where v = version tag
–all = hard SPF fail

The agency can incorporate additional optional attributes depending on their own requirements. For more information regarding the SPF record syntax review the following: http://www.openspf.org/SPF_Record_Syntax

3.4. Publish your SPF record, by working with your DNS server administrator.

3.5. Verify that your SPF record is correctly published. You can verify that the record was correctly published by using Agari's online tool at the following: https://www.agari.com/resources/tools/spf/

Accurately creating a valid SPF and DMARC record for all second-level domains is crucial to the success of protecting citizens and government employees from email-based attacks. Reviewing the DMARC aggregate and/or forensics reports provide an accurate view as to which internal and 3rd party senders are successfully aligning with your email authentication policies. It will be critical to continually monitor the DMARC reports to ensure you do not exclude valid senders.

4. Secure Sockets Layer (SSL) v2 and SSL v3 are disabled for mail servers

There are known critical security vulnerabilities in SSLv2 and SSLv3. To prevent these vulnerabilities from being exploited both SSL versions must be disabled. Disabling SSLv2 and SSLv3 on a mail server will vary depending on what software components are installed on the system. To meet the required actions, agencies should complete the following:

4.1. Catalog all applications currently enabled and running on the system.

4.2. For SMTP, SSLv2 and SSLv3 are typically used for email encryption e.g. STARTTLS. When configuring STARTTLS ensure that SSLv2 and SSLv3 are prevented from use. Refer to the mail server documentation to disable SSLv2 and SSLv3 for email encryption use.

4.3. When disabled, review the mail server logs to verify that SSLv2 and/or SSLv3 are not being used during the SMTP transaction.

Mail servers may also be running other applications to support services such as IMAP,

POP3, VPN, or Web. Refer to the documentation of those applications to disable and test that the server is not running SSLv2 and/or SSLv3.

5. 3DES and RC4 cryptographic ciphers are disabled on mail servers

There are known critical security vulnerabilities in 3DES and RC4 cryptographic ciphers. To prevent these vulnerabilities from being exploited both cipher types must be disabled for use. To meet the required actions, agencies should complete the following:

5.1. Catalog all applications currently enabled and running on the system.

5.2. For SMTP, 3DES and RC4 are used as the SSL ciphers for STARTTLS. When configuring STARTTLS ensure that 3DES and RC4 are prevented from use. Refer to the mail server documentation to disable 3DES and RC4 for email encryption use.

5.3. When disabled, review the mail server logs to verify that 3DES and RC4 are not being used during the SMTP transaction.

Mail servers may also be running other applications to support services such as IMAP, POP3, VPN, or Web. Refer to the documentation of those applications to disable and test that the server is not using 3DES and RC4 for SSL/TLS.

6. Set DMARC policy of "p=reject" for all second-level domains and mail-sending hosts.

Achieving a DMARC policy of "p=reject" is the end goal for implementing DMARC, an enforcement policy protects citizens and government employees against email-based attacks that attempt to impersonate Federal agencies. When the agency initially publishes a valid SPF and DMARC record as indicated in section 3, the agency should continue to monitor their DMARC reports to verify that only legitimate email is authorized for delivery and to continue to discover new senders. Prior to moving the DMARC policy from "p=none" to "p=reject" customer should conduct the following:

6.1. Conduct on-going review of DMARC aggregate and/or forensic reports for each domain to discover new senders and verify that the known valid IPs or 3rd party senders are successfully aligned.

6.2. For valid senders that are not successfully aligned, agencies should work internally and with those 3rd party senders to develop the correct strategy for alignment. Many 3rd party senders support aligned-SPF however it will be critical to work with these 3rd parties to verify support.

For example, many Federal agencies use GovDelivery as a 3rd party sender. GovDelivery supports aligned-SPF and provide instructions on how to include their GovDelivery Communications Cloud into your SPF record.

Agari works with 100's of well-known senders including GovDelivery. For assistance in discovery or instructions on how to align with 3rd party senders, contact us at: https://www.agari.com/federal-dmarc-consultation.

6.3. If new valid senders are discovered and support aligned-SPF, update your SPF record to include these senders. Changes to the SPF record should look similar to the following:

6.3.1. For sending domains, at minimum, the SPF record should look like the following:

v=spf1 ip4:x.x.x.x ~all
where v = version tag
ip4:x.x.x.x = valid IP addresses that are authorized to send mail (list all that apply)
~all = soft SPF fail

6.3.2. For domains where an authorized 3rd party sender is configured to send on the agencies' behalf, an 'include' attribute should be added to the SPF record. The 'include' attribute should be recorded similar to the following:

v=spf1 ip4:x.x.x.x include:_spf.3rdpartyexample.com ~all
where v = version tag
ip4:x.x.x.x = valid internal IP address that are authorized to send mail
include:_spf.3rdpartyexample.com = valid reference to authorized IP's or domains of the authorized 3rd party
~all = soft SPF fail

6.3.3. Publish your SPF record, by working with your DNS server administrator.

6.3.4. Verify that your SPF record is correctly published. You can verify that the record was correctly published by using Agari's online tool at the following: https://www.agari.com/resources/tools/spf/

6.4. Finally, when all 3rd party senders have been authorized, update your DMARC record to change the policy from "p=none" to "p=reject".

6.4.1. A change in the record should look similar to the following:

Before:
v=DMARC1; p=none; rua=mailto:agency@rua.agari.com

After:
v=DMARC1; p=reject; rua=mailto:agency@rua.agari.com

6.4.2. Work with your DNS server administrator to publish your DMARC record.

6.4.3. Verify that the record was successfully published
by using the Agari online tool at the following:
https://www.agari.com/resources/tools/dmarc/

7. National Cybersecurity & Communications Integration Center (NCCIC) added as a recipient of aggregate reports
When available, the NCCIC will require receipt of DMARC aggregate reports for their review and analysis. Once the NCCIC provides a valid email address to send DMARC aggregate reports, the agency's DMARC record will need to be updated. Agencies should complete the following steps to complete this requirement:

7.1. Update your DMARC record to include the provided NCCIC email address. The new DMARC record should look similar to the following:

Before:
v=DMARC1; p=reject; rua=mailto:agency@rua.agari.com

After:
v=DMARC1; p=reject;rua=mailto:agency@rua.agari.com,mailto:NCCICreportingaddress@example.gov

7.2. Work with your DNS server administrator to publish your DMARC record. Verify that the record was successfully published by using the Agari online tool at the following: https://www.agari.com/resources/tools/dmarc/

Required Actions – Web Security

8. All publicly accessible Federal websites & web services provide services through a secure connection (HTTPS-only with HSTS)

Data transferred across an HTTP connection is highly susceptible to being monitored, modified, or impersonated because the channel is unencrypted. To protect citizens and government employees from Internet-based attacks, all publicly accessible Federal websites and web services must enforce HTTPS with HSTS. HTTP Strict Transport Security will require that browsers connecting to these websites and services connect via (https://) regardless if the user enters (http://). In addition, HSTS eliminates the ability for users to click through certificate-related warnings. In order to meet the requirement, agencies should complete the following steps:

8.1. Catalog all publicly accessible Federal websites and web services.

8.2. For each website and web service, a typical configuration change may include the following:

8.2.1. Obtain, install, and activate a valid SSL certificate on the web server hosting the website or service.

8.2.2. Change the website or service's configuration file e.g. add 'Header always set Strict-Transport-Security' to the configuration and save the file.

Please note that configuring a website or service to use HSTS will vary from system to system, refer to the application's documentation for explicit instructions.

8.2.3. Verify that the website and/or service can only be accessible via an HTTPS connection.

Once enabled web browsers will automatically change any insecure request (http://) to secure requests (https://).

9. Secure Sockets Layer (SSL) v2 and SSL v3 are disabled for web servers

There are known critical security vulnerabilities in SSLv2 and SSLv3. To prevent these vulnerabilities from being exploited both SSL versions must be disabled. Disabling SSLv2 and SSLv3 on a web server will vary depending on what software components are installed on the server. To meet the required actions, agencies should complete the following:

9.1. Catalog all applications currently enabled and running on the system.

9.2. For HTTP, SSLv2 and SSLv3 are typically used to secure the client/server connection between browser and web server e.g. HTTPS with HSTS. When configuring HSTS ensure that SSLv2 and SSLv3 are prevented from use. Refer to the web server documentation to disable SSLv2 and SSLv3 for HSTS.

9.3. When disabled, review the web server logs to verify that SSLv2 and/or SSLv3 are not being used during the HTTP transaction.

Web servers may also be running other application to support service such as IMAP, POP3, VPN, or SMTP. Refer to the documentation of those applications to disable and test that the server is not running SSLv2 and/or SSLv3.

10. 3DES and RC4 cryptographic ciphers are disabled for web servers

There are known critical security vulnerabilities in 3DES and RC4 cryptographic ciphers. To prevent these vulnerabilities from being exploited both ciphers must be disabled. Disabling 3DES and RC4 on a web server will vary depending on what software components are installed on the server. To meet the required actions, agencies should complete the following:

10.1. Catalog all applications currently enabled and running on the system.

10.2. For HTTP, 3DES and RC4 are typically used to secure the client/server connection when using SSL/TLS e.g. HTTPS with HSTS. When configuring HSTS ensure that 3DES and RC4 ciphers are prevented from use. Refer to the web server documentation to disable 3DES and RC4 for HSTS.

10.3. When disabled, review the web server logs to verify that 3DES and/or RC4 ciphers are not being used during the HTTP transaction.

Web servers may also be running other application to support service such as IMAP, POP3, VPN, or SMTP. Refer to the documentation of those applications to disable and test that the server is not running 3DES and/or RC4.

11. Identify and provide a list of agency second-level domains that can be HSTS preloaded for which HTTPS will be enforced for all subdomains, to DHS

Web browsers e.g. Chrome, Firefox, Safari, Internet Explorer can maintain a preloaded list of second-level domains that will be enforced for HSTS by default. This means the browser will already be aware that the host requires use of SSL/TLS before any connection takes place. By default, when you configure all Internet-facing websites for HSTS, the associated domains and subdomains should be included in this list. However, you must ensure that the entire list of second-level domains is provided to DHS. To complete the required action, agencies should complete the following:

11.1. Catalog and create a list of all second-level domains that can be HSTS preloaded.

11.2. Email the list to DHS: FNR.BOD@hq.dhs.gov by February 13, 2018.

Status of Implementation

12. Submit to DHS - Report on the status of the BOD 18-01 Implementation

In order to meet this required action, agencies must:

12.1. Create a document which includes status and progress on each required action as documented in the 'Agency Plan of Action'. The Agency may use the Agari_BOD_1801_Plan_of_Action_TEMPLATE.pdf as a template to record on-going progress and active status.

12.2. Email the 'Agency Plan of Action Progress Report' to FNR.BOD@hq.dhs.gov by December 15, 2017.

12.3. **Submit to DHS – Subsequent reports on the status of the BOD 18-01 Implementation until completion**

To meet the required action, update the 'Agency Plan of Action Progress Report' with the latest progress and status and email to FNR.BOD@hq.dhs.gov every 30 days post December 15, 2017.

Roles and Responsibilities

In order to successfully meet the aggressive timelines associated with BOD 18-01, it is imperative that roles and responsibilities are defined prior to BOD 18-01 planning and implementation. Below is a sample list of relevant individuals who should be involved in the project. Depending on the structure of the agency the roles and responsibilities may be different.

Ref. #	Role/Team	Responsibilities
1	Executive Sponsor	Point of escalation for critical issues/project roadblocks
2	Project Owner	Responsible for overall success of the project
3	Project Manager	Responsible for ensuring that tactical milestones are being completed and schedules are being met
4	Implementation Team e.g. Messaging Administrator, Network Administrator, DNS Administrator, InfoSec Engineer	Responsible for execution of configuration changes, testing, and publishing DNS based changes
5	Vendor Project Manager/Customer Success Expert	3rd party assistance for implementation, if choosing to work with a 3rd party such as Agari

Optional Recommendations

1. Implementation of Domain Keys Identified Mail (DKIM) is currently not required to comply with BOD 18-01. While DKIM is technically not required to use DMARC, it is highly recommended. The use of DMARC, SPF, and DKIM offers the most comprehensive email authentication solution. DKIM defines a standardized way for agencies to digitally sign their email. This allows recipients to confirm with a high degree of assurance who the sender of the email really is, and whether or not the message was altered during transit.

2. Incorrectly configuring SPF and DMARC can have severe ramifications to Federal agencies in that malicious emails impersonating the agency are still delivered with the assumption that these emails are valid, and inadvertently blocking legitimate email, preventing critical Federal business communication. With the aggressive timelines associated with BOD 18-01, it is imperative to get the steps right the first time. Agari can help. To find out more contact us at https://www.agari.com/federal-dmarc-consultation.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.