Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Binding Operational Directive *BOD-18-01*
Original Release Date:
Applies to: All Federal Executive Branch Departments and Agencies

---

FROM: Elaine C. Duke
Acting Secretary

OCT 1 6 2017

CC: Mick Mulvaney
Director, Office of Management and Budget

SUBJECT: **Enhance Email and Web Security**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"). *Id.* § 3553(b)(2). Federal agencies are required to comply with these DHS-developed directives. *Id.* § 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. *Id.* § 3553(d)-(e).

I. Background

Federal agency 'cyber hygiene' greatly impacts user security. By implementing specific security standards that have been widely adopted in industry, federal agencies can ensure the integrity and confidentiality of internet-delivered data, minimize spam, and better protect users who might otherwise fall victim to a phishing email that appears to come from a government-owned system. Based on current network scan data and a clear potential for harm, this directive requires actions related to two topics: email security and web security.

A. Email Security

STARTTLS
When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does

not force the use of encryption, enabling STARTTLS makes passive man-in-the-middle attacks more difficult.

Email Authentication

Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) allow a sending domain to effectively "watermark" their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect. When an email is received that does not pass an agency's posted SPF/DKIM rules, Domain-based Message Authentication, Reporting & Conformance (DMARC) tells a recipient what the domain owner would like done with the message.

Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

B. Web Security

Hypertext Transfer Protocol (HTTP) connections can be easily monitored, modified, and impersonated; Hypertext Transfer Protocol Secure (HTTPS) remedies each of these vulnerabilities. HTTP Strict Transport Security (HSTS) ensures that browsers always use an https:// connection, and removes the ability for users to click through a certificate-related warning.

In 2015, OMB M-15-13 required all existing federal websites and web services to be accessible through a secure connection (HTTPS-only, with HSTS). In 2017, the .gov registry began automatically preloading new federal .gov domains as HSTS-only in modern browsers.[1]

Federal agencies must make more progress on HTTPS and HSTS deployment, including by removing support for known-weak cryptographic protocols and ciphers. According to DHS's cyber hygiene scanning data, seven of the ten most common vulnerabilities seen across federal agency networks at the issuance of this directive would be addressed through complying with the required actions in this directive related to web security.

II. Required Actions

All agencies are required to:

1) Within 30 calendar days after issuance of this directive, develop and provide to DHS an "Agency Plan of Action for BOD 18-01," according to the attached template, to:

[1] https://home.dotgov.gov/hsts-preloading/

a) Enhance email security:

i) Within 90 days after issuance of this directive, configuring:

- All internet-facing mail servers to offer STARTTLS, and
- All second-level agency domains to have valid SPF/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.

ii) Within 120 days after issuance of this directive, ensuring:

- Secure Sockets Layer (SSL)v2 and SSLv3 are disabled on mail servers, and
- 3DES and RC4 ciphers are disabled on mail servers.

iii) Within 15 days of the establishment of a centralized National Cybersecurity & Communications Integrations Center (NCCIC) reporting location, adding [NCATS domain] as a recipient of DMARC aggregate reports.

iv) Within one year after issuance of this directive, setting a DMARC policy of "reject" for all second-level domains and mail-sending hosts.

b) Enhance web security by:

i) Within 120 days after issuance of this directive, ensuring:

- All publicly accessible federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS)[2],
- SSLv2 and SSLv3 are disabled on web servers, and
- 3DES and RC4 ciphers are disabled on web servers.

ii) Identifying and providing a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.

2) Upon delivery of its Agency Plan of Action for BOD 18-01 within 30 days of this directive per required action 1, begin implementing that plan. If an agency expects to be unable to fully meet the above-provided deadlines, the agency should, within the Agency Plan of Action for BOD 18-01 due to DHS within 30 days of issuance of this directive, explain the challenges expected to cause the delay and how the agency plans to promptly overcome the challenges.

[2] https://https.cio.gov/

3) At 60 calendar days after issuance of this directive, 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.

III. DHS Actions

- DHS will review each Agency Plan of Action for BOD 18-01 after receipt and may contact agencies with concerns.
- DHS will coordinate the agency-provided lists of domains for HSTS preloading with DotGov.
- DHS will rely on scanning by its National Cybersecurity Assessments & Technical Services team for tracking and verifying progress with agency compliance with this directive.
- DHS will notify agencies when the NCCIC establishes a central location for the collection of agency DMARC aggregate reports, described above at II(1)(a)(iii).
- DHS will provide additional guidance through a DHS BOD coordination call and other engagements and products following the issuance of this directive.

IV. Potential Budgetary Implications

In general, DHS understands that compliance with BODs could result in budgetary implications. If agencies determine that such impacts exist during BOD implementation planning, agency Chief Information Officers and procurement officers should coordinate with the agency Chief Financial Officer, as appropriate.

V. DHS Point of Contact

Binding Operational Directive Team, FNR.BOD@hq.dhs.gov. All agency reports and plans related to this directive shall be sent to this address.

Attachment:

1. BOD 18-01 Plan of Action Template