OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

August 7, 2018

FROM: James Springs
Inspector General

TO: David S. Ferriero
Archivist of the United States

SUBJECT: NARA's Compliance with Binding Operational Directive 18-01 *(Special Report No. 18-SR-12)*

The purpose of this Special Report is to inform you of the progress the National Archives and Records Administration (NARA) is making toward compliance with the Department of Homeland Security's (DHS) Binding Operational Directive (BOD) 18-01.

Background

Security of federal websites significantly impacts website users. According to DHS improving federal website security through the implementation of security standards adopted by industry, allows federal agencies to ensure the integrity and confidentiality of internet-delivered data, minimize unsolicited email, and better protect users from phishing emails that appear to come from government-owned systems. DHS and the federal government are improving the security of government-owned systems including websites through the use of BODs.[1] One such BOD is 18-01, *Enhance Email and Web Security*.

BOD 18-01 is comprised of two components. The first is email security that requires agencies to implement STARTTLS[2] and improve email authentication by implementing Domain-based Message Authentication, Reporting & Conformance (DMARC). The second is a supplement to Office of Management and Budget's (OMB) Memorandum (M) 15-13, which requires all existing Federal websites and web services to be accessible through a secure connection (HTTPS-only, with HSTS). However, BOD 18-01 takes security a step further by requiring agencies to remove support for known-weak cryptographic protocols and ciphers.

Overall, NARA is making significant progress toward implementing BOD 18-01 with the .gov websites and emails. Based on the June 9, 2018 cyberhygiene[3] scans, NARA is 94% compliant

[1] According to DHS, BODs are compulsory direction to federal executive branch departments and agencies for purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.
[2] BOD 18-01 states STARTTLS is a protocol that signals to a sending mail server that the capability to encrypt an email in transit is present.
[3] Cyberhygiene scans are weekly scans (one for email compliance and another for website compliance) run by DHS to assist agencies in determining whether they are BOD 18-01 compliant.

with the website portion and 73% compliant with the email portion of the BOD. However, there are two categories, one in websites and one in emails, that are not incorporated into the compliance percentages as required. As a result, NARA cannot ensure the accuracy of the scan results indicating 94% of websites and 73% of emails are compliant with BOD 18-01.

Website Compliance with BOD 18-01

NARA is not ensuring all websites including those operated by a third party on behalf of NARA are compliant with BOD 18-01. NARA is not providing the appropriate oversight of its third-party websites. This is especially concerning considering NARA has several third party hosted websites that collect either proprietary or Personally Identifiable Information (PII). BOD 18-01 applies to internet-facing agency information systems, which encompasses those systems directly managed by an agency as well as those operated on an agency's behalf. BOD 18-01's primary focus is on agency mail and web infrastructure, regardless of domain suffix[4]. By not verifying all websites are compliant with BOD 18-01, NARA cannot ensure the confidentiality and integrity of internet-delivered data is protected for users of its websites.

In order to track implementation of this BOD, DHS requires agencies to provide a status report on a monthly basis. While NARA does report on their progress toward implementing BOD 18-01, they are only reporting on the results of DHS cyberhygiene scans performed on NARA's .gov websites. According to a GSA representative, these scans only cover some of what's in-scope of BOD 18-01 and OMB M-15-13. The representative goes on to say that it's ultimately up to an agency to identify what they have, and ensure secure connections are in place for all websites. As stated previously, the June 9, 2018 scan of NARA's environment indicated they were 94% compliant with the website portion of BOD 18-01. While these numbers indicate NARA has made significant progress toward implementing this directive, NARA is not providing DHS with its overall compliance with BOD 18-01 by only reporting the cyberhygiene results. Without tracking compliance over all NARA websites including third-party websites, NARA does not know if they are fully compliant with BOD 18-01.

Email Compliance with BOD 18-01

NARA is not ensuring all emails sent on behalf of the agency by third-party vendors are compliant with BOD 18-01. NARA is not providing the appropriate oversight of its venders that send emails on behalf of NARA. While DHS is reporting that NARA is 73% compliant as of June 9, 2018 with the email portion of BOD 18-01, this percentage does not include those vendors that send emails on behalf of NARA. According to NARA's Information Security personnel, there are two vendors currently sending emails on behalf of NARA. Information

[4] Federally operated domains do not all end in .gov, .mil, or .fed.us. Some may end in .com, .org, .us, or other suffixes. Any federally operated domain is covered by M-15-13. M-15-13 compliance guidance is required to be followed for the implementation of BOD 18-01.

Services is working to ensure the two vendors meet BOD 18-01 requirements. We noted there are other vendors who send emails on behalf of NARA that Information Services is not aware of. For example, NARA's Continuity of Operations Planning (COOP) vendor website sends emails on behalf of NARA to NARA employees notifying them when the COOP plan has been activated. Without ensuring all emails are compliant with BOD 18-01, NARA lacks assurance the integrity and confidentiality of such emails are maintained. We will continue to monitor NARA's progress toward fully implementing BOD 18-01.

Suggestions for Improvement

Information Services should:

1. Ensure all websites, government and contractor, identified during NARA's OMB 15-13 project are compliant with BOD 18-01.
2. Identify and document nara.gov email addresses that are sent from vendors on behalf of NARA.
3. Coordinate with the identified vendors and their government point of contact to identify and implement a solution for meeting BOD 18-01.

As with all OIG products, we will determine what information is publically posted on our website. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this report. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the Special Report.

Consistent with our responsibility under the *Inspector General Act, as amended*, we will provide copies of this report to congressional committees with oversight responsibility over the National Archives and Records Administration.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General for Audits, at (301) 837-3000.

cc: Deputy Archivist of the United States
Chief Information Officer
Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee