INSPECTION

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

THE DEPARTMENT OF THE INTERIOR GENERALLY COMPLIED WITH EMAIL AND WEB SECURITY REQUIREMENTS

Report No.: 2018-ITA-019

July 2018

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Memorandum

JUL 26 2018

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall Mary L Kendall
Deputy Inspector General

Subject: Final Inspection Report – The Department of the Interior Generally Complied with Email and Web Security Mandates
Report No. 2018-ITA-019

We completed our inspection of the U.S. Department of the Interior's compliance with secure communication requirements for publicly accessible web and email systems. Our inspection revealed that the Department was over 90 percent compliant with mandated security requirements, but we found areas where it needs improvement. Specifically, we found that the Department does not maintain its own inventory of publicly accessible websites, did not meet encryption requirements for the BisonConnect email service, and operated websites without the appropriate domain.

Background

The U.S. Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) established requirements to better protect the privacy of users and the confidentiality and integrity of Federal data. OMB Memorandum M-15-13[1], *Policy to Require Secure Connections across Federal Websites and Web Services*, required all Federal civilian publicly accessible websites to only provide service through a secure connection by December 31, 2016. DHS Binding Operational Directive (BOD) 18-01[2], *Enhanced Email and Web Security*, reinforced the OMB requirements with additional details and added security requirements for email services.

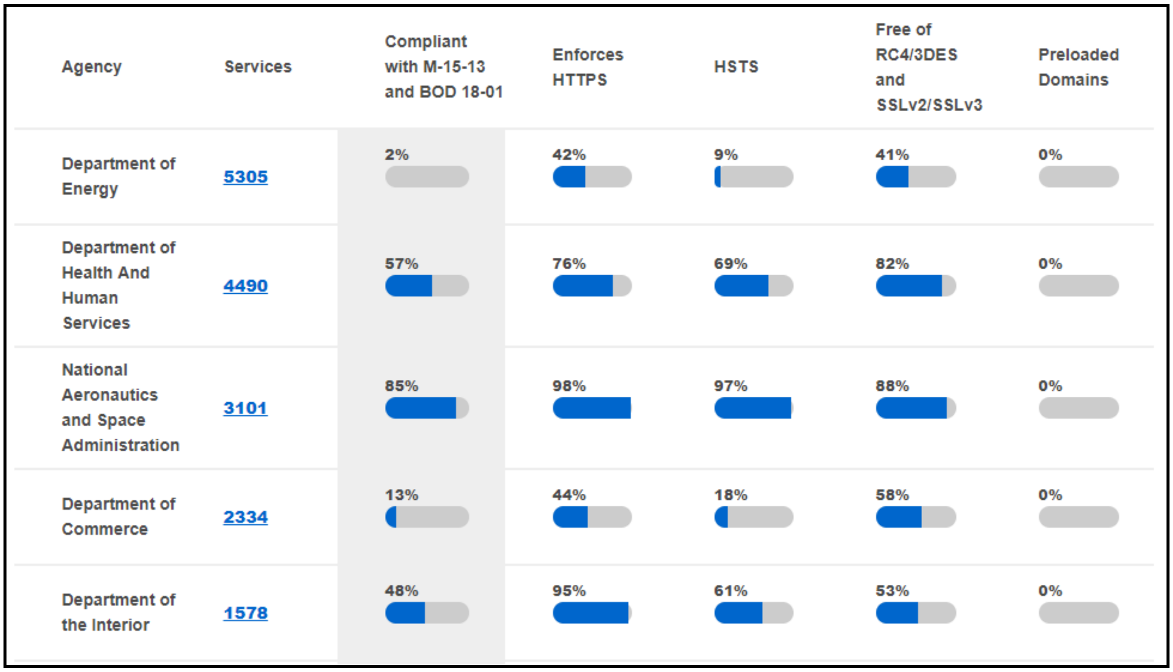
The deadlines for meeting the core requirements include:

- December 31, 2016 – initial website security compliance with OMB M-15-13
- February 13, 2018 – full website security compliance with DHS BOD 18-01
- January 15, 2018 – basic email security compliance with DHS BOD 18-01

[1] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf
[2] https://cyber.dhs.gov/assets/report/bod-18-01.pdf

- October 16, 2018 – full email security compliance with DHS BOD 18-01

The General Services Administration (GSA) performs periodic testing for these requirements and publishes governmentwide compliance results on the Pulse Dashboard (Pulse), available at https://pulse.cio.gov. Prior to OIG announcing this inspection in January 2018, the Department hosted the fifth most websites of all Federal civilian agencies and was 48 percent compliant with the DHS and OMB requirements (see Figure 1).



Agency	Services	Compliant with M-15-13 and BOD 18-01	Enforces HTTPS	HSTS	Free of RC4/3DES and SSLv2/SSLv3	Preloaded Domains
Department of Energy	5305	2%	42%	9%	41%	0%
Department of Health And Human Services	4490	57%	76%	69%	82%	0%
National Aeronautics and Space Administration	3101	85%	98%	97%	88%	0%
Department of Commerce	2334	13%	44%	18%	58%	0%
Department of the Interior	1578	48%	95%	61%	53%	0%

Figure 1: The Department was 48 percent compliant with the DHS and OMB requirements on December 24, 2018. Source: Pulse

We performed testing using different methods than GSA's, allowing us to generate more detailed reporting than is available from the Pulse dashboard. We performed tests to identify Department websites and email services, validate the results reported on Pulse, and evaluate websites and email services that are not tested by the GSA or reported on Pulse. While our testing confirmed similar overall compliance percentages, and the exact compliance status of each website tested, the results we generated cannot be directly compared to those reported on Pulse due to our different testing and reporting methodology.

Additional information on our scope and methodology can be found in Attachment 1 and a glossary of terms can be found in Attachment 2. We also provided information on our tools, as well as our scan and test results to the Office of the Chief Information Officer (OCIO).

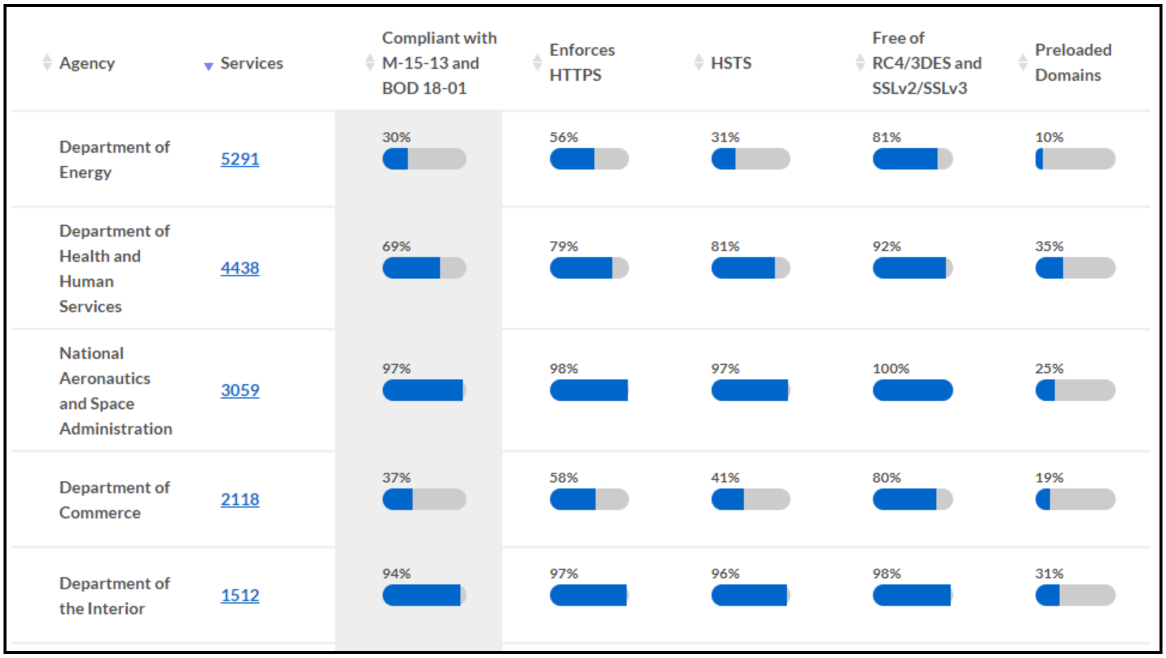
Findings

While our inspection revealed that the Department was over 90 percent compliant with the mandated security requirements, we found that the Department does not have an inventory of publicly accessible websites, did not meet encryption requirements for email service, and operated websites with unapproved top-level domain (TLD) names of ".net" and ".org" instead of the required ".gov" domain name.

Improved Security Compliance for Websites Reported on Pulse Dashboard

We found that 92 percent of the Department websites we tested were compliant with the mandated security requirements. Our overall test results matched closely with the Pulse reported results (94 percent). This demonstrated that the Department actively responded to the reports published on Pulse and worked to resolve noncompliant systems. Prior to announcing our inspection, the Department was 48 percent compliant with these requirements in December 2017 (as shown in Figure 1). Since announcing our inspection in January 2018, however, the Department improved its compliance to 94 percent – almost doubling the number of publicly accessible websites providing enhanced security and privacy.

The Department relied on the GSA and the DHS to test compliance of its websites. At the end of our inspection, the Department continued to host the fifth most number of websites of all Federal civilian agencies and had increased its compliance rating on Pulse to 94 percent (see Figure 2). Our testing validated this significant improvement.



Agency	Services	Compliant with M-15-13 and BOD 18-01	Enforces HTTPS	HSTS	Free of RC4/3DES and SSLv2/SSLv3	Preloaded Domains
Department of Energy	5291	30%	56%	31%	81%	10%
Department of Health and Human Services	4438	69%	79%	81%	92%	35%
National Aeronautics and Space Administration	3059	97%	98%	97%	100%	25%
Department of Commerce	2118	37%	58%	41%	80%	19%
Department of the Interior	1512	94%	97%	96%	98%	31%

Figure 2: The Department was 94 percent compliant with the DHS and OMB requirements on April 23, 2018. Source: Pulse

No Inventory of Publicly Accessible Websites

We found 357 publicly accessible websites that were not reported on Pulse. These additional websites consist of websites accessible by fully qualified domain names (FQDN) not known to the GSA, and websites that are accessible directly by Internet Protocol (IP) addresses or hosted on nonstandard ports. The tool used by the GSA is not capable of testing websites accessed via IP address or over nonstandard ports. Our testing of these unknown websites found only a 48 percent compliance with the DHS and OMB requirements (see Figure 3). These noncompliant systems pose an increased risk to the privacy of users and the confidentiality and integrity of Department data.

Type of website not reported on Pulse (includes non standard ports)	Number of websites not tested	Number not compliant	Percent Not Compliant
FQDN	153	79	52%
IP	204	93	46%
Total	**357**	**172**	**48%**

Figure 3: Of the 357 websites not reported on Pulse, 48 percent were not compliant with the secure website requirements.[3]

Websites tested and reported on Pulse are based on inventories provided by Federal agencies and by searching publicly accessible sources. Rather than create a comprehensive inventory of publicly accessible websites throughout the Department, the OCIO relied on Pulse and internal DHS reports. This led to missing websites and IP ranges from Department inventories. As a result, 357 websites were not tested, reported, and brought into compliance by the Department. The sites that did not meet the requirements have a greater risk of leaking sensitive data and communications with users since they use weak and flawed encryption. The scope of our work did not include vulnerability testing on the 357 missing public websites to determine potential risk of compromise from the presence of critical- and high-severity vulnerabilities. As such we could not assess the overall risk to the confidentiality, integrity, and availability of Department IT systems and data from the 357 missing websites.

Encryption Requirements Not Met for BisonConnect

We found that the Department implemented the Domain-based Message Authentication, Reporting and Conformance (DMARC) requirements for 134 of the 144 identified email domains (93 percent). In addition, we found that four email domains were ahead of schedule and already configured with requirements not due until October 2018.

The BisonConnect email service, however, was not compliant with web or email encryption requirements. Specifically, it was not compliant with the secure website requirement to disable 3DES, a weak form of encryption. BisonConnect is a contractor-managed email solution using Google's G-Suite for Government to provide the Department with a communication and collaboration tool. As of April 20, 2018, the OCIO's service request with the contractor responsible for the system was still awaiting implementation.

[3] This data includes a subset of 72 websites hosted on nonstandard ports, of which 51 (71 percent) were not compliant. The GSA does not identify, test, or report websites that are not hosted on either port 80 or port 443.

According to the Department's *Privacy Impact Assessment for BisonConnect*, "BisonConnect will be used Department-wide by all employees, contactors, volunteers, and others who have an official email account with DOI or any of DOI's bureaus, agencies, and offices." Until the contractor makes the configuration change, users' security and privacy on the Department's primary email system is vulnerable to compromise from malicious actors (e.g., greater success of compromising computers via phishing attacks).

Government Websites Operated Without the Appropriate Domain

We found that the Department operated 20 websites that did not use the .gov TLD, which contributed to the number of unidentified websites that are not being tested regularly. OMB's M-17-06[4], *Policies for Federal Agency Public Websites and Digital Services*, requires that Government websites only use the .gov TLD. These 20 websites used a mix of .org and .net TLD and were operating without waivers having been submitted to OMB. At least four of the domains did not belong to the Department at the time of testing, despite being configured in the Department's Domain Name System (DNS). In addition, seven of the domains were anonymously registered, which prevented us from determining site ownership using public records.

We believe the Department's processes for deploying new websites will prevent this from happening in the future. The non-compliant TLDs appear to be leftover configurations existing prior to the OMB TLD requirement. Misconfigurations like this can occur when there is no inventory to validate the configurations. Operating websites on non-.gov domains can reduce public confidence in Government websites because the public has no way of knowing whether the website is legitimate. In addition, these sites are more likely to contain unmitigated technical vulnerabilities because they are overlooked by security testing procedures, such as those reported on Pulse.

Recommendations

We recommend that the OCIO:

1. Develop a comprehensive inventory management program that includes periodic discovery scanning for all publicly accessible websites and IP ranges, including those with non-.gov domains.

2. Evaluate the websites we discovered for compliance with OMB and DHS web security requirements and submit the missing websites to the GSA for inclusion.

3. Periodically compare official inventory with Pulse and submit missing sites to GSA.

4. Conduct periodic scanning and reporting of websites that the GSA is unable to test.

5. Hold the contractor responsible for implementing BisonConnect accountable for complying with governmentwide mandates within the established deadlines.

[4] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf

6. Verify that each non .gov website or domain we identified either has a waiver or is migrated to a .gov domain.

We will forward these recommendations to the Office of Policy, Management and Budget for resolution and to track their implementation.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please contact me at 202-208-5745.

Attachments (2)

Scope and Methodology

Scope

The scope of this inspection included all publicly accessible websites and email systems operated by the Department of the Interior. We conducted data calls, documentation reviews, and technical testing. We performed technical testing between February 14, 2018, and March 13, 2018.

Methodology

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

To accomplish our inspection objectives, we:

- Conducted interviews with subject matter experts at the Office of the Chief Information Officer (OCIO) and conducted a data call
- Reviewed documentation provided by the OCIO including its implementation plan, web and Internet Protocol (IP) address inventories, Domain Name System (DNS) records, and firewall rule configurations
- Searched public resources for Department-owned IP addresses and websites, including the American Registry for Internet Numbers (ARIN)
- Developed custom tools for discovering and testing Department website and email configurations
- Analyzed the results of our technical tests

Technical Testing Details

Our tests were designed to test all publicly accessible websites operated by the Department. Our technical testing was performed in several phases, including discovery; web Secure Sockets Layer (SSL) testing; and email Domain-based Message Authentication, Reporting and Conformance (DMARC) testing. We did not test for the STARTTLS criteria because the Department's primary email solution permits weak ciphers. Until these ciphers are disabled, its encryption options such as STARTTLS will not meet compliance criteria. We developed custom tools to perform the technical testing because the tools made available by the General Services Administration (GSA) and the Department of Homeland Security (DHS) could not test all websites operated by the Department.

Discovery

We used the IP address inventories, website inventories, and DNS records provided by the Department to perform initial discovery scans. We also searched the ARIN database to identify additional IP addresses owned by the Department that were not included in the inventories provided. We analyzed the Department’s firewall rulesets to identify 92 open ports that could potentially host a website.

Our discovery scans tested every IP, network range, and port previously identified. This produced a list of host/port pairs that could be further tested for SSL compliance.

SSL Tests

Our tools were written to allow us to test sites that the GSA could not. This also allowed us to validate that different scanning tools would come to the same compliance with greater detail. For example, the tools used by the GSA were limited to standard ports 80 and 443. The GSA also did not test websites that were hosted directly by IP address instead of by domain name.

In addition, the GSA tools used a different testing and reporting methodology than our tools. The GSA tested each domain in four different ways (e.g., for the domain doi.gov, the following were tested: http://doi.gov:80, https://doi.gov:443, http://www.doi.gov:80, and https://www.doi.gov:443) but still counted it as a single site. For websites hosted on a cluster of servers, the results as posted to Pulse did not report the individual compliance status for each server but still counted it as a single site. Our tools reported compliance status for each host and port pair individually instead of combining them into a single host.

The differences in testing and reporting methodology makes it difficult to directly compare the results reported on Pulse to our own results.

DMARC Tests

We used the Department’s DNS records to identify all domains configured with mail exchanger (MX) records, indicating they were email domains. We performed separate DMARC tests on the list of domains configured with MX records because it included several that were not hosting websites, and therefore was not included in the list of websites we scanned for SSL compliance.

Attachment 2

Glossary

SSL – Secure Sockets Layer is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication. The SSL standard has been superseded by Transport Layer Security (TLS) and is no longer approved for use on Government websites.

FQDN – Fully Qualified Domain Name. Websites are typically accessed by their FQDN (e.g. https://cscsurvey.nbc.gov/).

IP Address – Internet Protocol (IP) Address. This is the numerical address of any network connected device. Websites can sometimes be accessed by this address instead of FQDN (e.g., https://137.227.224.120)

MX Records – Mail exchanger records. These are configurations that specify the email server(s) responsible for accepting email messages.

DNS – Domain Name System. DNS is a naming system for computers. This system is used to map FQDNs to IP addresses. It is also used to assign MX records for domains.

DMARC – Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations.

Nonstandard Ports – Websites typically operate on the standard port 80 for unencrypted web, and port 443 for encrypted web. Websites on a different port number are considered nonstandard and that port number is visible in the URL (e.g., https://www.oha.doi.gov:8080).

TLD – Top-Level Domain. Refers to the last segment of a domain name, or the part that follows immediately after the “dot” symbol. Examples of some of the popular TLDs include .com, .org, .net, .gov, .biz and .edu.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doioig.gov

By Phone:

24-Hour Toll Free:	800-424-5081
Washington Metro Area:	202-208-5300

By Fax: 703-487-5402

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240