April 14, 2015

Tony Scott
U.S. Chief Information Officer
Office of Management & Budget
1650 Pennsylvania Avenue, NW
Eisenhower Executive Office Building
Washington, DC 20503

By email to: https@cio.gov

RE: The HTTPS-Only Standard

Dear Mr. Scott,

You have sought public comment on the proposed “HTTPS-Only Standard,” which would require the use of HTTPS transport encryption on all publicly accessible federal websites and web services.¹ The American Civil Liberties Union (“ACLU”) welcomes this new policy, as well as the recognition by your office that “the American people expect government websites to be secure and their interactions with those websites to be private.”²

Although we are generally supportive of your proposal, as we describe in greater detail below, we believe that this deadline is not soon enough for some sensitive sites, such as those used by inspectors general, at least twenty-nine of which do not currently use HTTPS to protect reports of waste, fraud or abuse submitted via their internet hotlines. These include the inspectors general in the Departments of Justice and Homeland Security. We recommend that these sites be immediately upgraded to HTTPS.

Moreover, while HTTPS by default is a great first step, agencies should be employing other encryption best practices too, such as making sure that their email servers support the use of STARTTLS transport encryption.

---

¹ See https://https.cio.gov/
² Id.
HTTPS should be used for all content

For far too long, many in the technology industry incorrectly believed that HTTPS was only necessary to protect the submission of sensitive information, such as credit card and social security numbers. As such, many websites used unencrypted HTTP by default (and in many cases, redirected visitors who attempted to visit a HTTPS version of the site back to HTTP).

HTTPS does a lot more than protect the submission of sensitive information. It protects information about which web pages on a site a user is visiting and protects content submitted by the user or delivered by the site from tampering en-route. As a result, HTTPS can protect website visitors from so-called “man-in-the-middle attacks” in which their computers are infected with malware.

Default HTTPS is now an industry best practice

Over the past few years, default HTTPS has increasingly become the norm. Large technology companies such as Google, Facebook, Yahoo, and Twitter have all protected their sites with HTTPS by default, prodded in part by federal agencies and public officials. During the past year, major news organizations and several large law firms have also followed suit. Although largely motivated by a desire to protect user data from interception, as evidence has surfaced that unencrypted connections are being leverage by sophisticated actors to deliver malware, cyber

---

3 Morgan Marquis-Boire, You Can Get Hacked Just by Watching This Cat Video on YouTube, The Intercept (Aug. 15, 2014), https://firstlook.org/theintercept/2014/08/15/cat-video-hack/ (“Any unencrypted traffic can be maliciously tampered with in a manner that is invisible to the average user.”).
4 Id.
6 Facebook, Search Browsing by Default (July 31, 2013), https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920
security is now also a motivating factor. As one widely respected security engineer observed last year, “[unencrypted] cleartext [data] is no longer reasonable.”

Even before the announcement of the proposed “HTTPS-Only Standard”, a number of federal agency websites used HTTPS by default, including the Central Intelligence Agency, the National Security Agency, Healthcare.gov, and, most recently, the Federal Trade Commission, and the White House.

Some federal websites should be moved to HTTPS immediately

While we are supportive of your proposal to move all publicly accessible federal websites to HTTPS by default, we believe that the two-year timeline is not soon enough for some sensitive sites. These websites should be migrated to HTTPS as soon as possible.

For example, at least twenty-nine inspectors general surveyed by the ACLU do not currently use HTTPS to protect sensitive information submitted through their online “hotlines.” These include USAID, the Department of Agriculture, Amtrak, the Appalachian Regional Commission, the Architect of the Capitol, the Consumer Product Safety Commission, the Corporation for National & Community Service, the Corporation for Public Broadcasting, the Department of Agriculture, Amtrak, the Appalachian Regional Commission, the Architect of the Capitol, the Consumer Product Safety Commission, the Corporation for National & Community Service, the Corporation for Public Broadcasting, the Department of Agriculture, Amtrak.

12 Adam Langley, HTTP/2 and Proxies 8, IETF 90 (July 2014), https://www.ietf.org/proceedings/90/slides/slides-90-httpbis-0
14 Ashkan Soltani, FTC.gov is Now HTTPS by Default, FTC blog (Mar. 6, 2015), https://www.ftc.gov/news-events/blogs/techftc/2015/03/ftcgov-now-https-default
15 https://twitter.com/WHWeb/status/575509388133335041
16 See http://oig.usaid.gov/content/oig-hotline
18 See http://www.amtrakcoig.gov/content/report-allegation-fraud-waste-or-abuse
19 See http://ig.arc.gov/
20 See http://www.aoc.gov/oig/hotline
21 See http://www.cpsc.gov/cgbin/jiform.aspx (This website displays a “Norton Secured” logo which falsely suggests that all information submitted via the site will be encrypted in transit).
22 See http://www.cnqsoig.gov/complaint-form/complaint-and-disclosure-form
Assistance Commission, the Federal Housing Finance Agency, the Federal Labor Relations Authority, the Federal Maritime Commission, the General Services Administration, the Department of Homeland Security, the United States International Trade Commission, the Department of Justice, the Legal Services Corporation, the National Archives, the National Endowment for the Humanities, the National Labor Relations Board, the National Science Foundation, the Office of Personnel Management, the Postal Regulatory Commission, the U.S. Small Business Administration, the Smithsonian, the Special Inspector General for Afghanistan Reconstruction, the Special Inspector General for the Troubled Asset Relief Program, the Department of the Treasury, and the Treasury Inspector General for Tax Administration.

When individuals use these official whistleblowing channels to report waste, fraud or abuse, the information they submit is transmitted insecurely over the internet where it can be intercepted by others. This not only puts the identity of whistleblowers at risk, but also the confidentiality of the information they provide to inspectors general.

Similarly, the State Department operates a “Rewards for Justice” website through which individuals can report tips to help the U.S. government catch terrorists. Information submitted through the “submit a tip” form on this website is not encrypted.

That these sites do not use HTTPS to protect the submission of sensitive information (and likely have never used it) raises serious questions regarding the technical competence of the respective inspectors general and their ability to adequately protect sensitive information from cyber threats.

---

23 See http://www.cpb.org/oig/contact.php
25 See http://fhfaoig.gov/ReportFraud
26 See http://www.fira.gov/OIG-FILE_A_COMPLAINT
28 See http://www.gsaig.gov/index.cfm/hotline/-hotline-form/
29 See http://www.oig.dhs.gov/hotline/hotline.php
30 See http://www.usitc.gov/oig/hotline/ig_hotline
31 See http://www.justice.gov/oig/hotline/index.htm
33 See http://www.archives.gov/oig/referral-form/index.html
34 See http://www.neh.gov/about/oig/hotline-form
35 See http://www.nlrb.gov/who-we-are/inspector-general/inspector-general-hotline
36 See http://www.nsf.gov/oig/hotline_form.jsp
38 See http://www.prc.gov/contact-oig
39 See http://web.sba.gov/oigcss/client/dsp_welcome.cfm
40 See http://www.si.edu/OIG/HotlineForm
42 See http://www.sigtarp.gov/pages/hotline.aspx
43 See http://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx
44 See http://www.treasury.gov/tigta/contact_report.shtml#theform
45 See http://www.rewardsforjustice.net/english/submit-a-tip.html
threats. Moreover, many of these agencies have a Chief Information Security Officer, whose staff should have discovered and fixed this basic, yet critical, oversight. The responsible agencies should start moving these sites to HTTPS immediately.

**Agencies should make it easy, not difficult for the public to anonymously access their sites**

Although moving to HTTPS by default is a great first step, it will not address the leakage of certain metadata, such as the mere fact that someone is visiting a particular US government website. While the fact that an American is visiting the White House or IRS website is likely not sensitive, the fact that an agency employee, contractor or member of the public is visiting an inspector general website is. Similarly, the mere fact that someone in Pakistan or Yemen is visiting the Rewards for Justice website could be extremely sensitive and might even put their life at risk. Indeed, the Central Intelligence Agency, which has long used HTTPS by default for its site, warns foreigners visiting its website about this very issue:

> While we employ numerous safeguards to help minimize this risk, we suggest that you not use your home or work computer to contact us. Use instead a computer where you are entirely unknown. Although our website is encrypted, it is still possible for others to see that you have visited CIA.gov.  

A possible solution to the metadata leakage problem exists in the form of the Tor Project, a privacy enhancing technology initially created by the U.S. Naval Research Lab and subsequently funded by the Department of Defense and the Department of State, among other sponsors.

Currently, several federal agency websites block visitors who are using Tor. This practice should be changed. We recommend that you issue clear guidance prohibiting agencies from blocking access to visitors who are attempting to preserve their privacy and anonymity by using Tor. We also recommend that you encourage inspectors general to add information to their home pages informing visitors that they can download Tor and use it to hide their subsequent visits to the site.

In the longer term, we also recommend that federal websites that solicit sensitive information, such as inspectors general, deploy a secure, anonymous whistleblowing platform like Secure

---

46 See Central Intelligence Agency, Contact CIA, https://www.cia.gov/cgi-bin/comment_form.cgi (last visited Apr. 14, 2015) (text only shown to visitors with a non-US IP address).  
49 These include the Army (http://www.army.mil) and the FISA Court (http://www.fisc.uscourts.gov) (last visited Apr. 14, 2015)
Drop. This software is already used by many respected news organizations, including the Washington Post, the New Yorker and Forbes.

**Agencies should also embrace other encryption best practices**

In addition to mandating the use of HTTPS encryption to protect interactions with government websites, we recommend that you also require agencies to use a similar encryption technology, STARTTLS, to protect data transmitted between email servers. This decade-old encryption standard is now widely used by the private sector, including by major technology and telecommunications companies such as Google, Comcast, Microsoft, Verizon and Yahoo.

Although some federal agencies have configured their email servers to use STARTTLS, some have not, including the Federal Bureau of Investigation, the Federal Trade Commission, the Federal Communications Commission, NASA and the Department of Labor.

We would be happy to answer any questions you have, and would be happy to discuss any of the issues we describe in this comment with your staff.

Thank you,

Michael W. Macleod-Ball
Acting Director
Washington Legislative Office

Christopher Soghoian, Ph.D.
Principal Technologist
Speech, Privacy & Technology Project
csoghoian@aclu.org

---

54 See https://starttls.info/check/ftc.gov
55 See https://starttls.info/check/fcc.gov.
56 See https://starttls.info/check/nasa.gov
57 See https://starttls.info/check/dol.gov