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

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

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.[3] As a result, HTTPS can protect website visitors from so-called "man-in-the-middle attacks" in which their computers are infected with malware.[4]

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,[5] Facebook,[6] Yahoo,[7] and Twitter[8] have all protected their sites with HTTPS by default, prodded in part by federal agencies and public officials.[9] During the past year, major news organizations and several large law firms have also followed suit.[10] 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.*

[5] Sam Schillace, *Default HTTPS Access for Gmail*, Official Gmail Blog (Jan. 12, 2010), http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html; Danny Sullivan, *Post-PRISM, Google Confirms Quietly Moving to Make All Searches Secure, Except For Ad Clicks*, Search Engine Land (Sept. 23, 2013), http://searchengineland.com/post-prism-google-secure-searches-172487

[6] Facebook, *Search Browsing by Default* (July 31, 2013), https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920

[7] Jeff Bonforte, *HTTPS Now Default in Yahoo Mail*, Yahoo! Mail (Jan. 7, 2014), http://yahoomail.tumblr.com/post/72588816144/https-now-default-in-yahoo-mail

[8] Twitter, *Securing Your Twitter Experience With HTTPS* (Feb. 13, 2012), https://blog.twitter.com/2012/securing-your-twitter-experience-with-https

[9] Pamela Jones Harbour, FTC Commissioner, *Remarks Before Third FTC Exploring Privacy Roundtable* 7 (Mar. 17, 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-third-federal-trade-commission-exploring-privacy-roundtable/100317privacyroundtable.pdf ("security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using SSL by default. That includes all email providers, social networking sites, and any website that transmits consumer data. Step up and protect consumers."). *See also* Press Release*, Schumer: Wireless Network Connections at Coffee Houses and Bookstores Allow Easy Access to Hackers* (Feb. 28, 2011), https://web.archive.org/web/20121128134023/http://schumer.senate.gov/record.cfm?id=331455

[10] Eitan Konigsburg, Elena Kvochko and Rajiv Pant, *Embracing HTTPS*, N.Y. Times, Nov. 13, 2014, http://open.blogs.nytimes.com/2014/11/13/embracing-https/. *See also* Jonathan Randles*, Firms Move to Encryption to Quell Cybersecurity Fears*, Law360 (Mar. 16, 2015), http://www.law360.com/articles/630920/firms-move-to-encryption-to-quell-cybersecurity-fears

security is now also a motivating factor.[11] As one widely respected security engineer observed last year, “[unencrypted] cleartext [data] is no longer reasonable.”[12]

Even before the announcement of the proposed “HTTPS-Only Standard”, a number of federal agency websites used HTTPS by default,[13] including the Central Intelligence Agency, the National Security Agency, Healthcare.gov, and, most recently, the Federal Trade Commission,[14] and the White House.[15]

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,[16] the Department of Agriculture,[17] Amtrak,[18] the Appalachian Regional Commission,[19] the Architect of the Capitol,[20] the Consumer Product Safety Commission,[21] the Corporation for National & Community Service,[22] the Corporation for Public Broadcasting,[23] the Election

[11] Barton Gellman, *U.S. Firm Helped the Spyware Industry Build a Potent Digital Weapon for Sale Overseas*, Wash. Post, Aug. 15, 2014, http://www.washingtonpost.com/world/national-security/spyware-tools-allow-buyers-to-slip-malicious-code-into-youtube-videos-microsoft-pages/2014/08/15/31c5696c-249c-11e4-8593-da634b334390_story.html (“After Marquis-Boire disclosed to them confidentially last month that their services are under active attack, Google and Microsoft began racing to close security holes in networks used by hundreds of millions of users…. Since learning of Marquis-Boire’s findings in mid-July, Google has encrypted a majority of YouTube video links, and Microsoft has changed default settings to prevent unencrypted log-ins on most live.com services.”). *See also* Alexis C. Madrigal, *The Inside Story of How Facebook Responded to Tunisian Hacks*, The Atlantic (Jan. 24, 2011), http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/ (“First, all Tunisian requests for Facebook were routed to an https server. The Https protocol encrypts the information you send across it, so it's not susceptible to the keylogging strategy employed by the Tunisian ISPs.”).

[12] Adam Langley, *HTTP/2 and Proxies* 8, IETF 90 (July 2014), https://www.ietf.org/proceedings/90/slides/slides-90-httpbis-0

[13] Eric Mill, *Why We Use HTTPS for Every .gov We Make*, 18F (Nov. 13, 2014), https://18f.gsa.gov/2014/11/13/why-we-use-https-in-every-gov-website-we-make/; Eric Mill, *The First .gov Domains Hardcoded into Your Browser as all-HTTPS*, 18F (Feb. 9, 2015), https://18f.gsa.gov/2015/02/09/the-first-gov-domains-hardcoded-into-your-browser-as-all-https/

[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

[17] *See* http://www.usda.gov/oig/hotline.php

[18] *See* http://www.amtrakoig.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/cgibin/igform.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.cncsoig.gov/complaint-form/complaint-and-disclosure-form

Assistance Commission,[24] the Federal Housing Finance Agency,[25] the Federal Labor Relations Authority,[26] the Federal Maritime Commission,[27] the General Services Administration,[28] the Department of Homeland Security,[29] the United States International Trade Commission,[30] the Department of Justice,[31] the Legal Services Corporation,[32] the National Archives,[33] the National Endowment for the Humanities,[34] the National Labor Relations Board,[35] the National Science Foundation,[36] the Office of Personnel Management,[37] the Postal Regulatory Commission,[38] the U.S. Small Business Administration,[39] the Smithsonian,[40] the Special Inspector General for Afghanistan Reconstruction,[41] the Special Inspector General for the Troubled Asset Relief Program,[42] the Department of the Treasury,[43] and the Treasury Inspector General for Tax Administration.[44]

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.[45]

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

[23] *See* http://www.cpb.org/oig/contact.php
[24] *See* http://www.eac.gov/inspector_general/fraud_waste_and_abuse_form.aspx
[25] *See* http://fhfaoig.gov/ReportFraud
[26] *See* http://www.flra.gov/OIG-FILE_A_COMPLAINT
[27] *See* http://www.fmc.gov/resources/reporting_fraud_waste_and_abuse.aspx
[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
[32] *See* http://www.oig.lsc.gov/hotline_form/hotline.aspx
[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
[37] *See* http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse/complaint-form/
[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
[41] *See* http://www.sigar.mil/investigations/hotline/index.aspx?SSR=3&SubSSR=17&WP=Hotline
[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. [46]

A possible solution to the metadata leakage problem exists in the form of the Tor Project,[47] 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.[48]

Currently, several federal agency websites block visitors who are using Tor.[49] 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).

[47] *See* Tor Project, https://www.torproject.org (last visited Apr. 14, 2015)

[48] *See* Tor Project, *Sponsors*, https://www.torproject.org/about/sponsors.html.en (last visited Apr. 14, 2015)

[49] These include the Army (http://www.army.mil) and the FISA Court (http://www.fisc.uscourts.gov) (last visited Apr. 14, 2015)

Drop.[50] This software is already used by many respected news organizations, including the Washington Post, the New Yorker and Forbes.[51]

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.[52] Although some federal agencies have configured their email servers to use STARTTLS, some have not, including the Federal Bureau of Investigation,[53] the Federal Trade Commission,[54] the Federal Communications Commission,[55] NASA[56] and the Department of Labor.[57]

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

[50] *See* Secure Drop, https://securedrop.org/ (last visited Apr. 14, 2015)
[51] *See* Secure Drop, *The Official Secure Drop Directory*, https://freedom.press/securedrop/directory (last visited Apr. 14, 2015)
[52] *See* Google, *Transparency Report* http://www.google.com/transparencyreport/saferemail/#region=019 (last visited Apr. 14, 2015)
[53] *See* https://starttls.info/check/ic.fbi.gov and https://starttls.info/check/fbi.gov.
[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