Making HTTPS the default in the world's largest* bureaucracy

Eric Mill
Building the 21st century digital government.
Making government & politics more accountable & transparent.

SPOTLIGHT

Influence at the DNC: More than 60 superdelegates are registered lobbyists

ELECTIONS 2016

LATEST FROM THE BLOG

AUG. 8, 2016, 3:55 P.M.
A closer look at the problem of open data policy that isn't open

AUG. 8, 2016, 2:06 P.M.
Help us find political dark money in your state
HTTPS-Everywhere for Government

Posted by Tony Scott on June 08, 2015 at 03:57 PM EDT

Today, the White House Office of Management and Budget (OMB) issued the HTTPS-Only Standard directive, requiring that all publicly accessible Federal websites and web services only provide service through a secure HTTPS connection.

Unencrypted HTTP connections create a vulnerability and expose potentially sensitive information about users of unencrypted Federal websites and services. This data can include browser identity, website content, search terms, and other user-submitted information. To address these concerns, many commercial organizations have already adopted HTTPS-only policies to protect visitors to their websites and services. Today’s action will deliver that same protection to users of Federal websites and services.
M-15-13: Require Secure Connections

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Tony Scott
Federal Chief Information Officer

SUBJECT: Policy to Require Secure Connections across Federal Websites and Web Services

This Memorandum requires that all publicly accessible Federal websites and web services only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).
This Memorandum requires that Federal agencies deploy HTTPS on their domains using the following guidelines.

- Newly developed websites and services at all Federal agency domains or subdomains must adhere to this policy upon launch.

- For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic should receive priority and migrate as soon as possible.

- Agencies must make all existing websites and services accessible through a secure connection [3] (HTTPS-only, with HSTS) by December 31, 2016.

- The use of HTTPS is encouraged on intranets [4], but not explicitly required.

To monitor agency compliance, a public dashboard has been established at pulse.cio.gov.
What HTTPS Does

HTTPS verifies the identity of a website or web service for a connecting client, and encrypts nearly all information sent between the website or service and the user. Protected information includes cookies, user agent details, URL paths, form submissions, and query string parameters. HTTPS is designed to prevent this information from being read or changed while in transit.

HTTPS is a combination of HTTP and Transport Layer Security (TLS). TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.

Browsers and other HTTPS clients are configured to trust a set of certificate authorities [2] that can issue cryptographically signed certificates on behalf of web service owners. These certificates communicate to the client that the web service host demonstrated ownership of the domain to the certificate authority at the time of certificate issuance. This prevents unknown or untrusted websites from masquerading as a Federal website or service.
What HTTPS Doesn’t Do

HTTPS has several important limitations. IP addresses and destination domain names are not encrypted during communication. Even encrypted traffic can reveal some information indirectly, such as time spent on site, or the size of requested resources or submitted information.

HTTPS only guarantees the integrity of the connection between two systems, not the systems themselves. It is not designed to protect a web server from being hacked or compromised, or to prevent the web service from exposing user information during its normal operation. Similarly, if a user’s system is compromised by an attacker, that system can be altered so that its future HTTPS connections are under the attacker’s control. The guarantees of HTTPS may also be weakened or eliminated by compromised or malicious certificate authorities.
HSTS
HTTP Strict Transport Security

- Agencies must make all existing websites and services accessible through a secure connection [3] (HTTPS-only, with HSTS) by December 31, 2016.

- The use of HTTPS is encouraged on intranets [4], but not explicitly required.

```
$ curl --head https://www.whitehouse.gov

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
X-Drupal-Cache: MISS
X-Content-Type-Options: nosniff
ETag: "1468905085-1"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```
1. Working for GSA
2. Technology policy in the US government
3. Creating a new policy
4. Progress and challenges
5. Some takeaways
I don’t represent or work for the White House
I work for the most exciting agency in the federal government.
Work/Life Balance and Wellness

We understand the balancing act between work and personal life. GSA helps restore the balance by offering family-friendly health and wellness benefits that give you flexibility and peace of mind. We offer the following:

- **Telework (mobile work)** is offered with forward-thinking telework policies and a nimble IT environment, allowing you to do work and access IT resources anywhere, anytime.
- **Innovative, open, & collaborative work spaces**
- **Flexible work schedules**
Key initiatives

Open Source Policy: The GSA open-source strategy is still in effect and I will continue to look for ways to double-down on this strategy. It was a good idea a year ago and remains a good idea now. Any solution developed using taxpayer dollars should be in the taxpayer’s domain (open source) and the code we develop should be shared under an open license so others may benefit from it. In addition, we will give priority to using open source software as we design new solutions.
Open source by default #73

konklone opened this issue on Mar 22 · 8 comments

konklone commented on Mar 22

(I'm Eric, an engineer at 18F, an office in the U.S. General Services Administration (GSA) that provides in-house digital services consulting for the federal government. I’m commenting on behalf of 18F; we’re an open source team and happy to share our thoughts and experiences. This comment represents only the views of 18F, not necessarily those of the GSA or its Chief Information Officer.)

The draft policy's introduction asks:

Would an “open source by default” approach that required all new Federal custom code to be released as OSS, subject to exceptions for things like national security, be more or less effective in [fueling innovation, lowering costs, benefitting the public, and meeting the operational and mission needs of covered agencies]?

Yes, an “open source by default” approach would more effectively meet the White House’s goals with this policy.
100% agree, Eric. Regarding the views of the GSA CIO (me), we moved to an open source-first strategy for the enterprise in August of 2014, confirmed it again in October of 2015, operate against it at the strategic enterprise level, project level and at the data layer. Open source-first is baked into the GSA IT DNA and is one of our core operating principles. Just in case anyone reading your blog post was curious. DAS
Tr0ub4dor & 3

- Uncommon (non-gibberish) base word
- Order unknown
- Caps?
- Common substitutions
- Numerals
- Punctuation

Difficulty to guess: EASY

2^18 = 3 days at 1000 guesses/sec

Plausible attack on a weak remote web service: yes, cracking a stolen hash is faster, but it is not what the average user should worry about.

Difficulty to remember: HARD

Was it trombone? No, troubador. And one of the Os was a zero? And there was some symbol...

Correct horse battery staple

- Four random common words

Difficulty to guess: HARD

2^44 = 550 years at 1000 guesses/sec

Difficulty to remember: You’ve already memorized it

Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Verifiers SHOULD NOT impose other composition rules (mixtures of different character types, for example) on memorized secrets.

Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically) unless there is evidence of compromise of the authenticator or a subscriber requests a change.
GSA Employees: GSA is a great place to work!
Office of E-Government & Information Technology

Information technology (IT) advancements have been at the center of a transformation in how the private sector operates—and revolutionized the efficiency, convenience, and effectiveness with which it serves its customers. The Federal Government largely has missed out on that transformation due to poor management of technology investments, with IT projects too often costing hundreds of millions of dollars more than they should, taking years longer than necessary to deploy, and delivering technologies that are obsolete by the time they are completed. We are working to close the resulting gap between the best performing private sector organizations and the federal government.

The Office of E-Government and Information Technology (E-Gov), headed by the Federal Government’s Chief Information Officer (CIO), develops and provides direction in the use of Internet-based technologies to make it easier for citizens and businesses to interact with the Federal Government, save taxpayer dollars, and streamline citizen participation.
2. Technology policy in the US government
TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the “Federal Information Security Management Act of 2002”.

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

“SUBCHAPTER III—INFORMATION SECURITY

§ 3541. Purposes

“The purposes of this subchapter are to—

“(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

“(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

“(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

“(4) provide a mechanism for improved oversight of Federal agency information security programs;

“(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for Federal information security problems;
### TABLE D-16: SUMMARY — RISK ASSESSMENT CONTROLS

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-5(2)</td>
<td>VULNERABILITY SCANNING</td>
<td>LOW: X, MOD: X, HIGH: X</td>
</tr>
<tr>
<td>RA-5(3)</td>
<td>VULNERABILITY SCANNING</td>
<td>LOW: X, MOD: X, HIGH: X</td>
</tr>
<tr>
<td>RA-5(9)</td>
<td>VULNERABILITY SCANNING</td>
<td>LOW: X, MOD: X, HIGH: X</td>
</tr>
<tr>
<td>RA-5(10)</td>
<td>VULNERABILITY SCANNING</td>
<td>LOW: X, MOD: X, HIGH: X</td>
</tr>
<tr>
<td>Number</td>
<td>Date</td>
<td>Title</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>SP 800-185</td>
<td>August 2016</td>
<td>DRAFT SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>SP 800-184</td>
<td>June 2016</td>
<td>DRAFT Guide for Cybersecurity Event Recovery</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>SP 800-183</td>
<td>July 2016</td>
<td>Networks of 'Things'</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://csrc.nist.gov/publications/detail/sp/800/183/faq">SP 800-183 FAQ</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>doi:10.6028/NIST.SP.800-183 [Direct Link]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Press Release</td>
</tr>
<tr>
<td>SP 800-180</td>
<td>February 2016</td>
<td>DRAFT NIST Definition of Microservices, Application Containers and System Virtual Machines</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>SP 800-178</td>
<td>December 2015</td>
<td>DRAFT A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>SP 800-177</td>
<td>March 2016</td>
<td>DRAFT Trustworthy Email</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td>Announcement and Draft Publication</td>
</tr>
<tr>
<td>SP 800-176</td>
<td>August 2015</td>
<td>Computer Security Division 2014 Annual Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://csrc.nist.gov/publications/detail/sp/800/176/faq">SP 800-176 FAQ</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>doi:10.6028/NIST.SP.800-176 [Direct Link]</td>
</tr>
<tr>
<td>(Draft)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Title</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Privacy Guidance</td>
<td>M-15-10, Focusing on Implementation to Drive Improvements</td>
<td>April 6, 2015</td>
</tr>
<tr>
<td>Federal Register</td>
<td>M-15-08, Implementation of the President’s Executive Order on Fair Pay and Safe Workplaces</td>
<td>March 6, 2015</td>
</tr>
<tr>
<td>FOIA</td>
<td>M-15-07, Establishment of a Diversity and Inclusion in Government Council</td>
<td>March 6, 2015</td>
</tr>
<tr>
<td>NDA</td>
<td>M-15-06, Planning for Agency Operations Involving the Department of Homeland Security During a Lapse in its Appropriations</td>
<td></td>
</tr>
<tr>
<td>No FEAR</td>
<td>M-15-05, 2015 Discount Rates for OMB Circular No. 94</td>
<td>January 21, 2015</td>
</tr>
<tr>
<td></td>
<td>M-15-02, Appendix C to Circular No. A-123, Requirements for Effective Estimation and Remediation of Improper Payments</td>
<td>October 20, 2014</td>
</tr>
</tbody>
</table>

- M-15-19, Improving Government Efficiency and Saving Taxpayer Dollars Through Electronic Invoicing (July 17, 2015) (3 pages, 1.16 mb)


- M-15-17, Native Youth Priorities for the FY 2017 Budget (July 9, 2015) (4 pages, 2.05 mb)

- M-15-16, Multi-Agency Science and Technology Priorities for the FY 2017 Budget (July 9, 2015) (5 pages, 2.35 mb)


- M-15-11, Fiscal Year 2017 Budget Guidance (May 1, 2015) (8 pages, 2.87 mb)
• M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services (June 8, 2015) (5 pages, 259 kb)


• M-15-11, Fiscal Year 2017 Budget Guidance (May 1, 2015) (8 pages, 2.87 mb)

M-15-19, Improving Government Efficiency and Saving Taxpayer Dollars Through Electronic Invoicing (July 17, 2015) (3 pages, 1.16 mb)


M-15-17, Native Youth Priorities for the FY 2017 Budget (July 9, 2015) (4 pages, 2.05 mb)

M-15-16, Multi-Agency Science and Technology Priorities for the FY 2017 Budget (July 9, 2015) (5 pages, 2.35 mb)


M-15-11, Fiscal Year 2017 Budget Guidance (May 1, 2015) (8 pages, 2.87 mb)
OMB Circular A-130, Managing Federal Information as a Strategic Resource

- Transmittal Memorandum #4, “Management of Federal Information Resources” (11/28/2000 - 23 pages, 323 kb) HTML or PDF

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Managing Information as a Strategic Resource

1. Introduction
2. Purpose
3. Applicability
4. Basic Considerations
5. Policy
   a. Planning and Budgeting
   b. Governance
   c. Leadership and Workforce
   d. IT Investment Management
   e. Information Management and Access
   f. Privacy and Information Security
   g. Electronic Signatures
   h. Records Management
   i. Leveraging the Evolving Internet
<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5450.1</td>
<td>CIO CHGE 1 GSA Delegation of Authority Manual (GSA IT)</td>
<td>The authorities for the CIO’s Delegation of Authority Manual were delegated by the Administrator to the Chief Information Officer (CIO) to the Deputy CIO and the Chief Information Security Officer.</td>
</tr>
<tr>
<td>7000.3</td>
<td>Information Technology Standards for Internal GSA Workplaces</td>
<td>This Order is in support of GSA’s initiative to create model workplaces that support collaboration, improve productivity and utilization, and reduce costs. GSA has developed a set of standards to ensure that internal workplaces can function and be managed as a shared resource. These operating principles have been established to provide consistent and standardized workplace protocols and IT configurations.</td>
</tr>
<tr>
<td>9297.1</td>
<td>GSA Data Release Policy</td>
<td>This Order provides GSA’s policy on releasing information relating to GSA employees, contractors, and others on whom GSA maintains information described in this document.</td>
</tr>
<tr>
<td>9297.2B</td>
<td>GSA Information Breach Notification Policy</td>
<td>This Order provides GSA’s policy on what actions should be taken when it is determined that Personally Identifiable Information (PII) has been compromised and employees and contractors need to be notified.</td>
</tr>
<tr>
<td>1000G</td>
<td>GSA Telecommunications Guide</td>
<td>This guide establishes the General Services Administration’s (GSA) guidance regarding the use of GSA-provided employee telecommunications equipment, systems and services to facilitate information sharing and communications inside and outside of the Agency for conducting Government business. This guide amplifies CIO 2165.2 GSA Telecommunications Policy.</td>
</tr>
<tr>
<td>IL-01</td>
<td>Policy for OAuth 2.0 Integration with GSA.gov Accounts</td>
<td>This Instructional Letter (IL) establishes GSA policies for OAuth 2.0 integration of GSA.gov accounts with third party services including but not limited to Websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.</td>
</tr>
</tbody>
</table>
Figure 2. Allowed OAuth 2.0 Access Scopes

<table>
<thead>
<tr>
<th>Access Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Info</td>
<td>View your email address; View basic information about your account, including name, public profile URL, photo, gender, birthdate, country, language, and timezone</td>
</tr>
<tr>
<td>Limited Access to Data and Files</td>
<td>Access Google+ features which are generally public.</td>
</tr>
</tbody>
</table>


d. Google Apps Script is a JavaScript cloud scripting language that facilitates the automation of routine tasks across Google Apps and third party services. All scripts are subject to GSA IT review to verify author; access scope; where the script resides (e.g., internal vs external); type of data accessed; and storage of accessed data.

1. Internally developed scripts are implicitly allowed but may be restricted pending results of the OCISO review.

2. Internally developed scripts shall follow GSA naming conventions – GSA_2 Letter Service/Staff Office Designation_Script Name (e.g., GSA_IS_Script Name).

3. Externally developed scripts are prohibited but may be allowed following OCISO review and approval.

4. OCISO shall develop a process to review and approve Google Apps Scripts (internal and external) within 30 days of the signing of this IL.

e. GSA IT shall provide training on safely accessing third party services with GSA.gov accounts and OAuth 2.0.
Subtitle D—Federal Information Technology Acquisition Reform

SEC. 831. CHIEF INFORMATION OFFICER AUTHORITY ENHANCEMENTS.

(a) IN GENERAL.—Subchapter II of chapter 113 of title 40, United States Code, is amended by adding at the end the following new section:

10 USC 11319.

“§ 11319. Resources, planning, and portfolio management

“(a) DEFINITIONS.—In this section:

“(1) The term ‘covered agency’ means each agency listed in section 901(b)(1) or 901(b)(2) of title 31.
Sections and Attachments

OMB Memorandum M-15-14: Management and Oversight of Federal Information Technology
Attachment A: Common Baseline for IT Management and CIO Assignment Plan
Attachment B: Definitions of Terms for the Purposes of this Guidance
Attachment C: Template for Agency Common Baseline Self-Assessment and Plan
Attachment D: Fiscal Year (FY) 2015 PortfolioStat
Attachment E: Investment and Portfolio Management Maturity Framework
Attachment F: Additional Agency Human Capital Plan Requirements
Attachment G: Related Forthcoming Policies Roadmap
Attachment H: Cross-Walk of FITARA Requirements
Attachment I: Summary of Agency Deadlines and Requirements
Attachment J: Common Acronyms and Abbreviations
Attachment K: Applying FITARA Common Baseline to Statistical Agencies and Units

Endnotes
Offices of Inspector General

- Independent branch of most federal agencies
- Reports to the agency head and to Congress
- Often operates entirely separately (DNS, email, etc.)
18F AND U.S. DIGITAL SERVICE OVERSIGHT

Subcommittee on Government Operations
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
Subcommittee on Information Technology
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
HEARING DATE: JUNE 10, 2016 9:30 AM | 2154 RAYBURN HOB
Has the Federal Information Security Management Act helped the state of the government’s IT security?

Rhodes: FISMA has helped because it gave a framework. It made information system management and security management something that everyone was held accountable for. That said, implementation is everything. If security people view FISMA as just a checklist, nothing is going to get done. If you’re expending a huge amount of energy trying to do your day-to-day operations, a lot of people are going to look at it as another piece of paperwork that has to be sent in.

It’s not that FISMA hasn’t helped or that it needs to be changed. It’s a function of the information collection and the oversight associated with it, which needs to be strong. It needs to not be viewed as a paper exercise or allowed to be used as a paper exercise. It is a matter of making sure people do not become complacent because they met their check box on FISMA.
technical policy debt
it’s not enough just to make a new policy
people have to care
you have to make them care
3. Creating a new policy
Why we use HTTPS for every .gov we make

November 13, 2014
Tagged / security / best practices / https /

by Eric Mill

The .gov in government websites carries a lot of weight. Citizens expect government websites to be secure, trustworthy, and reliable. Citizens expect anything they read on a .gov website to be official, and they expect any information they submit to that website — especially if they’re submitting personal information — to be sent safely and only to the government.

On today’s Internet, in today’s web browsers, HTTPS (https://) offers the strongest guarantee of reliable information and secure transmission.

That’s why 18F’s policy is to use HTTPS for every .gov website we make. 18F is an in-house government technology team that builds things for the rest of the U.S. federal government, and we’re committed to deploying HTTPS across all of our released websites.
Find Out Whether This Unkillable Tracker Is On Your Smartphone

1. Device sends an HTTP request.
2. Verizon injects an HTTP header (“X-UIDH”). It’s a temporary ID, hashed or HMACed with a key.
3. Destination website (or third party) receives HTTP request with injected header.
4. Website directs request to advertising exchange.
5. Advertisers on the exchange can issue a paid API call to Verizon.
6. Verizon maps the header to a temporary ID, and returns the ID and/or advertising segments.
Comcast Wi-Fi serving self-promotional ads via JavaScript injection

The practice raises security, net neutrality issues as FCC mulls Internet reforms.

by David Kravets - Sep 8, 2014 8:00am EDT
Federal sites leaked the locations of people seeking AIDS services for years

By Craig Timberg  November 7, 2014  Follow @craigtimberg

Two federal government Web sites that help people find AIDS-related medical services have begun routinely encrypting user data after years in which they let sensitive information -- including the real-world locations of site visitors -- onto the Internet unprotected.
Find Free, Fast, and Confidential Testing Near You

Enter ZIP Code or City, State

Search

Not Sure What Test You Need?
Answer a few questions and we'll help you.

What is your gender?

[ ] Male  [ ] Female  [ ] Transgender

Next
The first .gov domains hardcoded into your browser as all-HTTPS

February 9, 2015
Tagged / https / security / best practices /

by Eric MILL

```json
1778.  { "name": "uspsoig.gov", "include_subdomains": true, "mode": "force-https" },
1779.  { "name": "notalone.gov", "include_subdomains": true, "mode": "force-https" },
1780.  { "name": "aids.gov", "include_subdomains": true, "mode": "force-https" },
1781.  { "name": "itdashboard.gov", "include_subdomains": true, "mode": "force-https" },
1782.  { "name": "paymentaccuracy.gov", "include_subdomains": true, "mode": "force-https" },
1783.  { "name": "cao.gov", "include_subdomains": true, "mode": "force-https" },
1784.  { "name": "cfo.gov", "include_subdomains": true, "mode": "force-https" },
1785.  { "name": "cio.gov", "include_subdomains": true, "mode": "force-https" },
```

Every .gov website, no matter how small, should give its visitors a secure, private connection. Plain HTTP
Your browser may soon force you to connect securely to some U.S. government Web sites

By Andrea Peterson  February 11, 2015

Aids.gov is one of the government domains taking an extra step to keep visitors information private. (Aids.gov)
In another step to enhance the FTC’s website, I’m pleased to announce that our agency has enabled encryption by default (HTTPS) for ftc.gov, our primary public domain, and home of the Tech@FTC blog. Ironically, as I was preparing this post, the entire internet has been FREAKing out about another vulnerability in SSL.

While we have long provided secure transport for FTC domains that handle sensitive consumer data, such as complaint data and email subscriptions, consumers will now browse our entire site more privately, and their browsers will automatically verify the identity of the website to which they’re connecting – an important step to mitigate attempts to impersonate the FTC.
A .gov website that uses HTTPS encryption by default for its visitors is a superb example of “privacy by design.” On March 6th, the Federal Trade Commission enabled encryption for FTC.gov. When I visited whitehouse.gov tonight, I found that the White House digital team had flipped the site for what’s likely the most prominent government website in the world. The White House Web team confirmed the change just after midnight.
March 2015: Released for 30 days of public comment

The HTTPS-Only Standard

The American people expect government websites to be secure and their interactions with those websites to be private. Hypertext Transfer Protocol Secure (HTTPS) offers the strongest privacy protection available for public web connections with today’s internet technology. The use of HTTPS reduces the risk of interception or modification of user interactions with government online services.

This proposed initiative, “The HTTPS-Only Standard,” would require the use of HTTPS on all publicly accessible Federal websites and web services.

We encourage your feedback and suggestions.

Goal

All publicly accessible Federal websites and web services [1] only provide service over a secure connection.
Why HTTPS for Everything?

HTTP has become central to today’s way of life. HTTP is currently the primary protocol for applications used on computers, tablets, smartphones, and many other devices.

As our dependency on the internet has grown, the risk to users' privacy and safety has grown along with it.

Every unencrypted HTTP request reveals information about a user’s behavior, and the interception and tracking of unencrypted browsing has become commonplace.

Today, there is no such thing as non-sensitive web traffic, and public services should not depend on the benevolence of network operators.

When properly configured, HTTPS can provide a fast, secure connection that offers the level of privacy and reliability that users should expect from government web services.

Privacy and integrity by default
+1 on behalf of Google Chrome

OTI Public Comment: OTI Supports the Proposed HTTPS-Only Standard

Very excited to see this proposal

Secure-to-origin for CDNs

Advise secure cookies

EFF public comment: HTTPS-Only is necessary and overdue

Changes per IETF IAB comments

A much-needed bar-raising

+1 from X-Lab.

+1 from the W3C TAG
I'm thrilled to see this proposal! People deserve secure and private access to government documents. The bulk of industry has already shifted -- or is in the process of shifting -- to HTTPS, and the U.S. government should not lag behind. I look forward to downloading my 2016 tax documents over HTTPS instead of HTTP.
Everyone who cares about free speech should care about the attacks on Github

Updated by Timothy B. Lee on March 30, 2015, 6:20 p.m. ET   tim@vox.com
Why confidential tips to the government may not be confidential after all

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 Election 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.
HTTPS-Everywhere for Government

Posted by Tony Scott on June 08, 2015 at 03:57 PM EDT

Today, the White House Office of Management and Budget (OMB) issued the HTTPS-Only Standard directive, requiring that all publicly accessible Federal websites and web services only provide service through a secure HTTPS connection.

Unencrypted HTTP connections create a vulnerability and expose potentially sensitive information about users of unencrypted Federal websites and services. This data can include browser identity, website content, search terms, and other user-submitted information. To address these concerns, many commercial organizations have already adopted HTTPS-only policies to protect visitors to their websites and services. Today’s action will deliver that same protection to users of Federal websites and services.
Finalizing the HTTPS-Only Standard as formal policy #108

Merged konklone merged 15 commits into master from changes on Jun 8, 2015

Below are some details on the changes we've made since the original proposal. I've mapped some to commits, but some are lumped in to others.

- 725b141 - Emphasize that high-priority websites should begin the HTTPS migration process immediately, and set a specific deadline of December 31, 2016.
- 7f0836c - Elaborate on planning for change, mention cipher/protocol choices and forward secrecy explicitly.
- 6cb9a30 and eee26c9 - Incorporate the IETF's suggested revisions on integrity in #97, and then make further edits to relevant areas to clarify mixed content and SNI. Thanks to @josephlhall for the detailed pull request.
- e2061fe - A number of non-substantive copy changes, and rewording to reflect the transition from proposal to policy.

Thank you again to everyone who participated!

Fixes #78, fixes #79, fixes #80, fixes #81, fixes #83, fixes #84, fixes #86, fixes #87, fixes #88, fixes #89, fixes #92, fixes #93, fixes #94, fixes #95, fixes #96, fixes #97, fixes #98, fixes #99, fixes #100, fixes #101, fixes #103, fixes #104, fixes #105, fixes #106, and fixes #107.
Intro to HTTPS

Eric Mill, Gray Brooks
18F, GSA

https://www.whitehouse.gov

An Introduction to HTTPS (Beginner)
An Introduction to HTTPS Part II: Implementing HTTPS
Migrating to HTTPS

Eric Mill, 18F/GSA
Timothy Badaczewski, ICF International

Migrating .gov to HTTPS: Common Pain Points and Practical Advice

DigitalGov

Subscribe 1,299

46 views
HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS. HSTS exists to remove the need for the common, insecure practice of redirecting users from http:// to https:// URLs.

When a browser knows that a domain has enabled HSTS, it does two things:

- Always uses an https:// connection, even when clicking on an http:// link or after typing a domain into the location bar without specifying a protocol.

- Removes the ability for users to click through warnings about invalid certificates.

A domain instructs browsers that it has enabled HSTS by returning an HTTP header over an HTTPS connection.
Compliance FAQ

- What does “all Federal agency domains or subdomains” include?
- What about domains that are only used to redirect visitors to other websites?
- What about domains that are technically public, but in practice are only used internally?
- What happens to visitors using browsers that don’t support HSTS, like older versions of Internet Explorer?
- This site redirects users to HTTPS – why is Pulse saying it doesn’t enforce HTTPS?
- Are federally operated certificate revocation services (CRL, OCSP) also required to move to HTTPS?
- What if I’m using a federally issued certificate – such as from the Federal PKI or Department of Defense – for my web service?
Certificates

Frequently asked questions and answers about HTTPS certificates and certificate authorities.

- What are certificates and certificate authorities?
- What kind of certificate should I get for my domain?
- What rules and oversight are certificate authorities subject to?
- Does the US government operate a publicly trusted certificate authority?
- Are there federal restrictions on acceptable certificate authorities to use?
- Then how can I limit which CAs can issue certificates for a domain?
  - Certificate Transparency
  - HTTP Public Key Pinning
There were **2.03 billion** visits over the past 90 days.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>desktop</td>
<td>58.3%</td>
</tr>
<tr>
<td>mobile</td>
<td>35.6%</td>
</tr>
<tr>
<td>tablet</td>
<td>6.1%</td>
</tr>
</tbody>
</table>

Based on rough network segmentation data, we estimate that less than 5% of all traffic across all agencies comes from US federal government networks.

Much more detailed data is available in downloadable CSV and JSON. This includes data on combined browser and OS usage.

<table>
<thead>
<tr>
<th>Browsers</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>42.8%</td>
</tr>
<tr>
<td>Safari</td>
<td>25.3%</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>17.1%</td>
</tr>
<tr>
<td>11.0</td>
<td>14.2%</td>
</tr>
<tr>
<td>7.0</td>
<td>1.1%</td>
</tr>
<tr>
<td>9.0</td>
<td>0.7%</td>
</tr>
<tr>
<td>10.0</td>
<td>0.6%</td>
</tr>
<tr>
<td>8.0</td>
<td>0.4%</td>
</tr>
<tr>
<td>6.0</td>
<td>&lt; 0.1%</td>
</tr>
<tr>
<td>Other</td>
<td>&lt; 0.1%</td>
</tr>
<tr>
<td>Firefox</td>
<td>8.1%</td>
</tr>
<tr>
<td>Edge</td>
<td>3%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>49.6%</td>
</tr>
<tr>
<td>7</td>
<td>28.6%</td>
</tr>
<tr>
<td>10</td>
<td>14.4%</td>
</tr>
<tr>
<td>8.1</td>
<td>3.8%</td>
</tr>
<tr>
<td>XP</td>
<td>1.3%</td>
</tr>
<tr>
<td>Vista</td>
<td>0.8%</td>
</tr>
<tr>
<td>8</td>
<td>0.6%</td>
</tr>
<tr>
<td>Other</td>
<td>&lt; 0.1%</td>
</tr>
<tr>
<td>iOS</td>
<td>23.1%</td>
</tr>
<tr>
<td>Android</td>
<td>17.3%</td>
</tr>
<tr>
<td>Macintosh</td>
<td>8.4%</td>
</tr>
<tr>
<td>Other</td>
<td>1.7%</td>
</tr>
</tbody>
</table>
Pounding the pavement

- Support emails (lots of them)
- Traveling to agencies to talk to staff
- Working with GSA shared services
👋 The EPA is the first agency with > 1 .gov domain to hit 100% HTTPS + HSTS for all of them: pulse.cio.gov/https/domains/ ...
NCATS Overview

- Offer Full-Scope Red Team/Penetration Testing Capabilities through two primary programs: Risk and Vulnerability Assessment (RVA) and Cyber Hygiene
- Focus is on proactive engagements with stakeholders to improve their cybersecurity posture, limit exposure, reduce rates of exploitation
- Offers a full suite of tailored threat, vulnerability and risk assessment services and penetration testing capabilities to stakeholders
- Acts as a trusted advisor and provides independent review and recommendations for cybersecurity
Success Story: HeartBleed

Notable Observations:

- DHS had the capability to initiate scanning immediately but was delayed due to a lack of authorization.
- Observed 98% vulnerability reduction between first and last scan.
- Had scanning started April 7th and achieved similar results the length of exposure could have been reduced by 29%.
National Cybersecurity Assessments & Technical Services Team (DHS)

We hack governments (and others) to improve 'cyber hygiene'.

The Internet  https://www.dhs.gov/cy...

ncats_info@hq.dhs.gov
This comment represents only the views of NCATS, not necessarily those of the US Department of Homeland Security or its Chief Information Officer.

We are the National Cybersecurity Assessments & Technical Services (NCATS) team, a unit inside the Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC). NCATS concurs (and applauds!) the comments posted by the DHS CIO (#222).

Thank you for this opportunity to submit comments, and for extending the deadline.

To what extent is the proposed pilot an effective means to fuel innovation, lower costs, benefit the public, and meet the operational and mission needs of covered agencies?

As a federal team that includes software developers, penetration testers, and security analysts, NCATS supports any government initiative that enables technologists, federal or not, to reuse or enhance others’ work, especially to reduce cost and duplicative effort, speed the delivery of products and services, and solve hard, shared problems. Open sourcing government-produced or -procured software is an important way for the public to be more direct beneficiaries of the services they have paid for. It also enables direct collaboration and information sharing which, if engaged in transparently, creates trust. This trait, along with increased software security generally, is what we hope to see because of this action.
Pulse

How federal government domains are meeting best practices on the web.

52% USE HTTPS

49% PARTICIPATE IN THE DIGITAL ANALYTICS PROGRAM

VIEW HTTPS RESULTS

VIEW ANALYTICS RESULTS
Secure HTTP (HTTPS)
Last updated August 05, 2016

This data measures whether federal domains support the HTTPS protocol (https://), and the strength of that support. HTTPS provides a secure connection across the internet between websites and their visitors, and is becoming the new baseline for public web services. As part of this shift, the U.S. federal government is in the process of transitioning entirely to HTTPS.

Note that HTTPS generally does not affect whether a website is vulnerable to hacking. For more information on what HTTPS does (and doesn't do), visit the HTTPS FAQ.

HTTPS and TLS data was last collected through a scan of the public internet on August 05, 2016.
<table>
<thead>
<tr>
<th>Domain</th>
<th>Uses HTTPS</th>
<th>Enforces HTTPS</th>
<th>Strict Transport Security (HSTS)</th>
<th>SSL Labs Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>18f.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, and preloaded</td>
<td>A+</td>
</tr>
<tr>
<td>911.gov</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>B</td>
</tr>
<tr>
<td>abandonedmines.gov</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>abilityone.gov</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>abmc.gov</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>A</td>
</tr>
<tr>
<td>access-board.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>A-</td>
</tr>
<tr>
<td>acl.gov</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>B</td>
</tr>
<tr>
<td>acquisition.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>T</td>
</tr>
<tr>
<td>acus.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, and preloaded</td>
<td>A-</td>
</tr>
<tr>
<td>ada.gov</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, and preload-ready</td>
<td>A-</td>
</tr>
</tbody>
</table>

Showing 1 to 10 of 752 entries (filtered from 1,153 total entries)
4. Progress and challenges
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Required</th>
<th>Recommended</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses HTTPS</td>
<td>28%</td>
<td>52%</td>
<td>24%</td>
</tr>
<tr>
<td>Enforces HTTPS</td>
<td>15%</td>
<td>37%</td>
<td>22%</td>
</tr>
<tr>
<td>Strict Transport Security</td>
<td>3%</td>
<td>14%</td>
<td>11%</td>
</tr>
<tr>
<td>Preloading</td>
<td>1%</td>
<td>3%</td>
<td>2%</td>
</tr>
</tbody>
</table>

*pulse.cio.gov, July 2015 to August 2016, ~1,150 parent .gov domains, no subdomains, federal only (all branches)*
Having recently gotten the HTTP Observatory to a usable state, I decided to scan the Alexa Top 1M sites to see how well that engineers and developers on the biggest sites on the Internet are doing. As Scott found out, the results are pretty dismal. I’ll be doing more detailed posts on each of these sections as I find the time, but even the basic statistics are depressing.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Security Policy (CSP)</td>
<td>.005% / .012%</td>
</tr>
<tr>
<td>Cookies</td>
<td>42.05%</td>
</tr>
<tr>
<td>Cross-origin Resource Sharing (CORS)</td>
<td>93.78%</td>
</tr>
<tr>
<td>HTTPS</td>
<td>29.64%</td>
</tr>
<tr>
<td>HTTP → HTTPS Redirection</td>
<td>5.06% / 8.91%</td>
</tr>
<tr>
<td>Public Key Pinning (HPKP)</td>
<td>0.43%</td>
</tr>
<tr>
<td>— HPKP Preloaded</td>
<td>.414%</td>
</tr>
<tr>
<td>Strict Transport Security (HSTS)</td>
<td>1.75%</td>
</tr>
<tr>
<td>— HSTS Preloaded</td>
<td>.158%</td>
</tr>
</tbody>
</table>
No one has a complete list of .gov web services
A complete list of .gov domains

December 18, 2014
Tagged / open data / open government /

by Eric Mill and Gray Brooks

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>AFTONWYOMING.GOV</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>AG.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>53</td>
<td>AGAZ.GOV</td>
<td>State/Local Govt</td>
</tr>
<tr>
<td>54</td>
<td>AGINGSTATS.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>55</td>
<td>AGUACALIENTE-NSN.GOV</td>
<td>Native Sovereign Nation</td>
</tr>
<tr>
<td>56</td>
<td>AHCPR.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>57</td>
<td>AHRQ.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>58</td>
<td>AIDS.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>59</td>
<td>AIKENCOUNTYSC.GOV</td>
<td>County</td>
</tr>
<tr>
<td>60</td>
<td>AIRNOW.GOV</td>
<td>Federal Agency</td>
</tr>
<tr>
<td>61</td>
<td>AK.GOV</td>
<td>State/Local Govt</td>
</tr>
</tbody>
</table>

There are a lot of .gov domains: over 5,300 of them. About 1,300 of these are used by the federal government's executive, legislative, and judicial branches. The rest are spread across states, territories, counties, cities, and...
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Domain Type</th>
<th>Agency</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANFRANCISCO.GOV</td>
<td>City</td>
<td>General Services Administration</td>
<td>San Francisco</td>
</tr>
<tr>
<td>SF.GOV</td>
<td>City</td>
<td>General Services Administration</td>
<td>San Francisco</td>
</tr>
<tr>
<td>ABERDEENMD.GOV</td>
<td>City</td>
<td>Non-Federal Agency</td>
<td>Aberdeen</td>
</tr>
<tr>
<td>ABERDEENWA.GOV</td>
<td>City</td>
<td>Non-Federal Agency</td>
<td>Aberdeen</td>
</tr>
<tr>
<td>ABINGDON-VA.GOV</td>
<td>City</td>
<td>Non-Federal Agency</td>
<td>Abingdon</td>
</tr>
<tr>
<td>ABINGTONMA.GOV</td>
<td>City</td>
<td>Non-Federal Agency</td>
<td>Abington</td>
</tr>
</tbody>
</table>
Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [more information]
Enter an **Identity** (Domain Name, Organization Name, etc), a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**: (% = wildcard)

[Search](#)  [Advanced...](#)

© COMODO CA Limited 2015-2016. All rights reserved.
## Visits to and traffic sources for all participating agencies

<table>
<thead>
<tr>
<th>Description</th>
<th>Download</th>
<th>Update frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visits to all domains over 30 days</td>
<td>CSV</td>
<td>Daily</td>
</tr>
<tr>
<td>Top downloads yesterday</td>
<td>CSV</td>
<td>Daily</td>
</tr>
<tr>
<td>Top traffic sources (30 days)</td>
<td>CSV, JSON</td>
<td>Daily</td>
</tr>
<tr>
<td>Top exit pages (30 days)</td>
<td>CSV, JSON</td>
<td>Daily</td>
</tr>
<tr>
<td>All pages people are visiting</td>
<td>CSV</td>
<td>Every 3 minutes</td>
</tr>
<tr>
<td>Total people online</td>
<td>JSON</td>
<td>Every 3 minutes</td>
</tr>
</tbody>
</table>
HSTS is brand new to the federal space
HSTS
HTTP Strict Transport Security

- Agencies must make all existing websites and services accessible through a secure connection [3] (HTTPS-only, with HSTS) by December 31, 2016.

- The use of HTTPS is encouraged on intranets [4], but not explicitly required.

```
$ curl --head https://www.whitehouse.gov
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
X-Drupal-Cache: MISS
X-Content-Type-Options: nosniff
ETag: "1468905085-1"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```
so many intranet subdomains on domains in public DNS

- Agencies have had to undo preloading
- Shared services can’t blanket preload
lots of malformed HSTS headers
$ date
Fri Oct 23 02:00:03 EDT 2015

$ curl --head https://example.gov
Strict-Transport-Security: max-age=17330797;

$ date
Fri Oct 23 02:00:05 EDT 2015

$ curl --head https://example.gov
Strict-Transport-Security: max-age=17330785;
Enterprise PKI
Your connection is not private

Attackers might be trying to steal your information from www.iad.gov (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

- Automatically report details of possible security incidents to Google. Privacy policy

ADVANCED  
Back to safety
What if I’m using a federally issued certificate – such as from the Federal PKI or Department of Defense – for my web service?

There are no restrictions on acceptable certificate authorities agencies might use to meet the requirements of M-15-13.

However, M-15-13 requires agencies to do more than just redirect HTTP traffic to HTTPS. It also requires agencies to enable HTTP Strict Transport Security (HSTS), as described above. HSTS ensures that HTTPS is always used, and protects users from several common vulnerabilities.

One important effect of HSTS is that it disables the ability for users to click through certificate warnings in supporting browsers. This means that agencies cannot instruct users to click through certificate warnings to use their web service while also complying with M-15-13.

This is also consistent with security best practices, as instructing users to click through certificate warnings defeats the point of HTTPS, and will subject users to potential network attacks.
What about Federal PKI certificates?

- The Federal PKI is working to ensure the Federal Common Policy CA is recognized by all public trust stores.
- Working on alignment of Federal Common Policy Certificate Policy requirements with the CA/Browser Forum Baseline Requirements.
- They expect the Federal Common Policy CA will be included in the Mozilla public trust store by 2019.
- The process may take longer or shorter depending on the result of public discussion of the Federal PKI’s application.
people are weird about certificates
## Certificate Validation Types

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Example URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain (DV)</td>
<td>I’m 18f.gsa.gov</td>
<td><a href="https://www.google.com">https://www.google.com</a></td>
</tr>
<tr>
<td>Organization (OV)</td>
<td>I’m also 18F at GSA</td>
<td><a href="https://twitter.com">https://twitter.com</a></td>
</tr>
<tr>
<td>Extended (EV)</td>
<td>I’m also the government</td>
<td></td>
</tr>
</tbody>
</table>
free or inexpensive DV certificates are completely acceptable for government use
Enterprise inspection: still a thing
We need more stories and more (open source) software that point a different way forward than MITM
So much hard work
Web Service Documentation

Explore our available Web services.

- Broadcasting Board of Governors
- BusinessUSA.gov API
- Department of Agriculture
- Department of Commerce
- Department of Education
- Federal Communications Commission
- Federal Election Commission
- Food and Drug Administration
- General Services Administration
- National Aeronautics and Space Administration
- National Institutes of Health
- National Renewable Energy Laboratory
- Regulations.gov API

API Key

Sign up to use our APIs.

- Get an API Key

About This Service

api.data.gov is a free API management service for federal agencies. Our aim is to make it easier for agencies to release and manage APIs.

More information for agencies
Choose whether HTTPS is required to access this API. HTTPS is encouraged to protect the API keys.

- **Required & return message**: HTTPS is required to access the API. HTTP requests will return an error message instructing the user to use an HTTPS URL instead. This is the recommended and default strategy.

- **Required & return redirect**: HTTPS is required to access the API. HTTP requests will return a redirect to the HTTPS URL.

- **Transitional & return message**: New API keys that signup after choosing this setting will be forced to use HTTPS. Existing API keys may continue to use either HTTP or HTTPS. New API keys using HTTP will return an error message instructing the user to use an HTTPS URL instead.

- **Transitional & return redirect**: New API keys that signup after choosing this setting will be forced to use HTTPS. Existing API keys may continue to use either HTTP or HTTPS. New API keys using HTTP will return a redirect to the HTTPS URL.

- **Optional**: HTTPS is optional and either HTTP or HTTPS may be used.

*Notes on redirects:*

- Not all API clients will automatically follow redirects, so be careful if using a redirect strategy for existing APIs (since existing calls may break).

- If API clients rely on the redirect for HTTPS access, this strategy does not secure the API keys, since the client may still be making an insecure initial HTTP request with their API key.

- For GET requests a 301 Moved Permanently redirect will be returned. For all other HTTP methods a 307 Temporary Redirect redirect will be returned (to instruct the client to retry using the same HTTP method).
HTTPS at NCBI: Guidance for users of NCBI Web APIs

What is happening?
To improve security and privacy, and by Federal government mandate, NCBI is moving all of its Web sites and services, including Web APIs, to HTTPS only by September 30, 2016.

If you use NCBI only through a Web browser (like Safari, Firefox, Chrome, Internet Explorer, Opera, etc.), this document is not of interest to you. The only change you should notice after the deadline is that a green lock icon should appear inside the box, and the web addresses of the NCBI pages you visit will start with https://.

If you maintain software that uses NCBI APIs or accesses NCBI servers through the Web, you should understand and act before the deadline to ensure uninterrupted service.

NCBI Web services include APIs such as NCBI utilities and BLAST URLAPI that client applications use to access NCBI data. A number of them (though not a comprehensive set) are listed on or linked from our APIs page.

Applications that access NCBI web servers using http: URLs, instead of https:// URLs, may fail partially or completely after NCBI switches to HTTPS-only.

This document explains our transition plan, and provides guidance to developers about how to update their applications (scripts, server-side applications like CGIs, browser plugins, etc.), before the switchover, to prevent failure.

NCBI is moving all web services to HTTPS

The HTTP protocol does not provide encryption, so anyone who can see web traffic between a client (for example, a web browser) and a server can intercept potentially sensitive information, and/or inject malware into users' browsers or operating systems. HTTPS solves this problem. It works just like HTTP, except that traffic is encrypted in both directions, so observers between the client and the server can't intercept or tamper with the requests or responses. It also provides authentication, ensuring that the client is communicating with the intended server given by the hostname, and not some impostor.

The Federal Office of Management and Budget requires all Federal Web sites to switch to HTTPS-only (meaning, HTTP will be disabled) by December 31, 2016. However, NCBI, being a part of the National Library of Medicine, has an earlier deadline of September 30, 2016.
Share Your Thoughts on Strong Encryption | The White House

www.whitehouse.gov/webform/share-your-thoughts-onstrong-encryption

Thanks again for adding your name to the petition on supporting strong encryption. This week, White House administration officials will sit down with ...

HTTPS-Everywhere for Government | whitehouse.gov

www.whitehouse.gov/blog/2015/06/08/https-everywhere-government

HTTPS-Everywhere for Government. June 8, 2015 at 3:57 PM ET by Tony Scott Twitter Facebook Email .

Summary: Today, the White House Office of ...

Remarks by the President in a Conversation on the Supreme Court Nomination

www.whitehouse.gov/the-press-office/2016/04/08/remarks-president-conversation-supreme-court-nomi...

4 months ago - example is this whole debate around encryption, which I think is just the tip of
your concept ▪ our infrastructure ▪ your success
maybe Norway will do this
Hvor stor andel av domener eid av det offentlige i Norge bruker HTTPS?

Statlige

7% BRUKER HTTPS
251 / 3.697

Lokale og regionale

5% BRUKER HTTPS
287 / 5.803
Nasjonal sikkerhetsmyndighet
Postboks 814
1306 SANDVIKA

Nasjonal sikkerhetsmyndighet

Vår saksbehandler
2016-05-25

Vår dato
2016-04-01

Vår referanse
A03 - S:16/01408-2

Deres dato
16/2346 - ROKO

Deres referanse
Side

Antall vedlegg
1 av 3
Oppdrag NSM - sikker tilkobling; HTTPS


NSM har utarbeidet en rapport om bruk av HTTPS i for offentlige tjenester. Rapporten er vedlagt dette svaret i sin helhet og utdyper emnet ytterligere.

Vurdering av hensiktsmessigheten av å innføre krav om sikker tilkobling til statlige webtjenester

NSMs anbefaling

NSM mener at alle offentlige tjenester på web alltid skal benytte HTTPS. Dette vil gi både

Tilsvarende anbefalinger fra andre nasjoner

NSM er kjent med at amerikanske og tyske myndigheter har innført krav om bruk av HTTPS i offentlig forvaltning. I USA kravstilte Office of Management and Budget i memorandum av 8.
5. Some takeaways
so much more HTTP left to get rid of
President Obama Opens 'American Idol' Finale, Urges Americans to Vote

“So go to Vote.gov and register today.”
we need to make it
a plain HTTP preload list
preloading .gov

(requires state, local, tribal)
we should push TLDs to require HTTPS going forward
(enforced by preloading)
we have to pay down technical policy debt

- Be willing to retract outdated policies
- Literally refactor everything
- Post internal policies publicly
- Solicit public comment on internal policies
- Making compliance costs proportionate to the risk
proactive, public, positive

- People want to be part of something great
- Even compliance monitoring should be celebratory
- Active public shaming is a failure state
- Agencies need to talk about their technical work
- Don’t wait on other people, keep doing things
for folks on the outside

- Your comments matter
- You have to show up (because others will)
- Speaking to those outside your community of practice
- Empowering people on the inside to win arguments
or you could join the inside!
Office of Technology Research and Investigation

The Office of Technology Research and Investigation (OTech) is located at the intersection of consumer protection and new technologies. As a trusted source for research and information on technology's impact on consumers, the Office conducts independent studies, evaluates new marketing practices, and provides guidance to consumers, businesses and policy makers. It also assists the FTC's consumer protection investigators and attorneys by providing technical expertise, investigative assistance, and training. The Office is housed in the Bureau of Consumer Protection and its work supports all facets of the FTC's consumer protection mission, including issues related to privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, fraud, big data, and the Internet of Things.

For additional technology-related content, please visit the Tech@FTC blog.
Apply now
Tours of duty
Dress code
Compensation
Relocation
Background check
Benefits

The best of technology.
The best of government.
And we want you.

We're looking for the most tenacious designers, software engineers, product managers, and more, who are committed to untangling, rewiring and redesigning critical government services. You'll join a team of the most talented technologists from across the private sector and government.

Contact Information

First Name *
Making HTTPS the default in the world's largest* bureaucracy

Eric Mill