NC DIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

ROY COOPER
GOVERNOR

J. ERIC BOYETTE
SECRETARY & STATE CHIEF INFORMATION OFFICER

Memorandum

To: All Agency CIOs

From: Maria S. Thompson, State Chief Risk Officer
NC Department of Information Technology

Subject: Mandatory Use of HTTPS for Publicly Accessible Websites

Date: March 8, 2018

**** Please share this memo broadly within your organization. ****

The continued use of unencrypted HTTP protocol for State agency public websites creates an unnecessary risk to the protection of our citizens' data. The HTTP protocol is insecure and allows for malicious actors to eavesdrop, compromise privacy and modify the integrity of the citizens' data. While it is understood that some system contains only public data, the State needs to standardize its approach for the overall protection of all data types.

To address these concerns, industry partners supporting mainstream browsers such as Mozilla Firefox have indicated their intent to flag all HTTP sites as insecure. As providers of services for the State, we must ensure that our citizen-facing experience provides assurance of our dedication and ability to protect their data. As a note, sites that have been transitioned to the State's Digital Commons platform are compliant with this policy.

This memorandum requires all State agencies to transition to HTTPS no later than **July 31, 2018.** This transition will be accomplished in multiple phases as outlined in this document.

Project Timelines and Requirements:

Phase 1 - Discovery:

In an effort to help agencies identify the websites associated with their services, ESRMO has conducted a scan of sites configured to use the DIT Domain Name Service (DNS) infrastructure. This list will be provided to the agencies via separate correspondence. Note: This list is not inclusive of all state websites, ESRMO does not have visibility into websites that are either cloud hosted or that do not use the aforementioned DIT DNS infrastructure. Agencies must:

- Review the provided list of websites
- Develop a strategy for the decommissioning of obsolete sites (as applicable)
- Develop a migration strategy for the operational sites to be configured for HTTPS
- Provide the plan to the agency's Business Relationship Manager (BRM) **NLT May 30, 2018**

Phase 2 – Implementation/ Migration

The State understands that this transition may come at a cost to the agencies. The State also realizes that there may be unique situations with legacy sites that may require code rewrite. However, due to increased risks to our State's data, this has become a priority. Below is an estimate of the costs for SSL certificates. Note: The current SSL contract allows for volume discounts. The cost per certificates will decrease as purchases are made.

- Annual cost for SSL Certificates (**est.** $260)

Agencies with public facing websites containing **ONLY** public data and which have **NO** backend databases or interconnections with systems hosting restricted or highly restricted data, have the option of using an open source solution, "LetsEncrypt" to meet this requirement for secondary and redirect sites. This solution allows for the following services and capabilities:

- Domain validation
- Certificate issuance and revocation

All other websites must purchase SSL Certificates that allow for Domain Validation (DV), Organizational Validation (OV) or Extended Validation (EV), as applicable.

DIT Roles and Responsibilities:

To assist in the implementation phase, ESRMO has devised courses of actions that agencies may use to accomplish this task.

Courses of Action:

A. Fully Qualified Domain Names: (FQDN)

Web sites where the FQDN, (example: site.com and www.site.com) is registered with one or more top level domains, (TLD), e.g. ".net", ".com", ".org", ".gov"; example: site.com, site.org) can be configured to be the primary with the other sites setup to always redirect to the primary. For example, visitors to site.com would be automatically redirected to site.org. This enables the other lesser used domains to use the "LetsEncrypt" solution. The primary in this case will use the purchased SSL Certificate. Alternatively, a SSL Certificate can be purchased that covers all FQDNs but additional cost may apply.

B. Sub-Domains:

In the case of sub-domains, a consideration would be to consolidate under one domain where-by the sub-domain becomes a directory. For example, two fully qualified domain names (FQDN) of topic1.site.org and topic2.site.org could become site.org/topic1 and site.org/topic2. For a transition period, the original sub-domains would be setup to redirect to the new location and would be able to use "LetsEncrypt" while the primary site uses the purchased SSL Certificate. By monitoring the web logs of the redirected sub-domain FQDNs, an agency would be able to determine when they could be retired and thereby save any costs associated with them.

There are various ways to configure redirects, please refer to the sites' web server documentation. Also, remember to review the "Potential Constraints or Considerations" section for those domains that do and do not redirect.

All sites must be migrated to HTTPS **NLT July 31, 2018.** During this phase, agencies are also required to discontinue and remove obsolete websites

Phase 4 – Internet Applications

The completion date for this phase has not been determined. During this phase, agencies will be required to implement SSL on all applications served to the internet. DIT will provide additional guidance on requirements for SSL Offloading services. This service will allow ESRMO to inspect the SSL traffic for anomalous activities.

Agency Guidelines

The following items are provided to guide the agencies in the transition to HTTPS:

a) From the date of this memo, all newly developed or deployed public sites must be in compliance
b) Agencies, as part of their transition strategy, should prioritize sites using the following criteria:

1. Forward facing sites that support transactions for the transfer of sensitive data e.g. Personally Identifiable Information (PII), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act and others

2. Sites identified with high traffic volume

Potential Constraints or Considerations:

Site Performance: While encryption adds some computational overhead, modern software and hardware can handle this overhead without substantial deleterious impact on server performance or latency.[1] Websites with content delivery networks or server software that supports the SPDY or HTTP/2 protocols, which require HTTPS in some major browsers, may find their site performance substantially improved as a result of migrating to HTTPS.

Server Name Indication: The Server Name Indication extension to TLS allows for more efficient use of IP addresses when serving multiple domains. However, these technologies are not supported by some legacy clients. [2] Web service owners should evaluate the feasibility of using this technology to improve performance and efficiency.

Mixed Content[3]: Websites served over HTTPS need to ensure that all external resources (images, scripts, fonts, iframes, etc.) are also loaded over a secure connection. Modern browsers will refuse to load many insecure resources referenced from within a secure website. When transitioning sites, agencies should consider that there may be a need to support a combination of automated and manual updates, replacement, or removal of references to insecure resources.

[1] https://istlsfastyet.com/

[2] https://https.cio.gov/sni/

[3] https://https.cio.gov/mixed-content/

APIs and Services[4]: Web services that serve primarily non-browser clients, such as web APIs, may require a more gradual and hands-on migration strategy, as not all clients can be expected to be configured for HTTPS connections or to successfully follow redirects.

Strict Transport Security: Websites and services available over HTTPS must enable HTTP Strict Transport Security (HSTS)[5] to instruct compliant browsers to assume HTTPS going forward. This reduces the number of insecure redirects, and protects users against attacks that attempt to downgrade connections to plain HTTP.

Secure Cookies: Websites and services available over HTTPS that use cookies must enable the "secure flag"[6] within the cookie parameters to indicate that the cookie not be sent in clear text. This protects the cookie information from various attacks and malicious use.

Strength and Quality[7]: Where HTTPS is enabled the protocol version, ciphers, and SSL certificate used shall be configured to meet Statewide Information Security Manual policies and/or other applicable regulatory requirements that exceed State policies.

Change Control: Cyber threats and vulnerabilities are a revolving concern. Agencies must ensure that solutions selected take into consideration the timeliness for patch management and remediation efforts.

Communication Strategy & Roles and Responsibilities

1. The Digital Commons Team has developed a web presence that contains Frequently Asked Questions (FAQs) and other information to better educate citizens as well as State employees on the importance of the use of HTTPS. This information can be found at: https://it.nc.gov/why-https

2. DIT Communications Team will also assist in the campaign using social media and other platforms to further disseminate the information.

3. The DIT Business Relationship Managers will engage with agency business owners to assist in the workflow and processing of this task.

4. SSL Certificate purchase: ESRMO will support the purchase of certificates. Remedy tickets must be addressed through normal channels

5. Firewall modifications: DIT Operations will implement firewall changes from port 80 to port 443 from approved agency representatives

If you have any questions about this requirement, please contact State Chief Risk Officer Maria Thompson at maria.s.thompson@nc.gov or (919) 754-6578.

[4] https://https.cio.gov/apis/"Migrating APis"

[5] https://https.cio.gov/hsts, "Strict Transport Security"

[6] https://www.owasp.org/index.php/SecureFlag

[7] https://https.cio.gov/technical-guidelines/