December 19, 2016

Good day, thank you for composing the draft practice guide, "Domain Name Systems-Based Electronic Mail Security" accessed at: https://nccoe.nist.gov/sites/default/files/library/sp1800/dns-secure-email-sp1800-6-draft.pdf

I have reviewed the entire document, and pursuant to the opportunity to submit feedback on this draft, draw your attention to the following seven reproduced passages and corresponding comments:

- **Page 31, line 177-181**

"4.4.3 Risk

Risks are examined from the point of view of consequences of vulnerabilities being exploited. Some examples of these consequences include legal liability, consequences of failure to comply with regulations, confidentiality breaches, loss of productivity, and damage to organizational reputation."

Comment: Another example of consequence may be "damage to the perceived value of an organization," to be distinguished from organizational reputation, which is more about the habits or characteristics of a particular organization. Please see: https://www.wired.com/2016/10/security-news-week-verizon-reportedly-wants-1-billion-discount-yahoo-deal/ and http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports/ . "The discount is being pushed because it feels Yahoo's value has been diminished, sources said."

- **Page 35, Data security, lines 318-329**

"a. **PR.DS-1**

The **PR.DS-1** subcategory under Data Security supports protection of data at rest. The user-to-user digital signature capability demonstrated by the DNS-Based E-Mail Security project can provide an ability to verify the source and content integrity of stored e-mail messages where the digital signature is stored with the rest of the message. This supports integrity protection for data-at-rest.

b. **PR.DS-2**

The **PR.DS-2** subcategory under Data Security supports protection of data in transit. In addition to user-to-user digital signature of e-mail, the DNS-Based E-

Mail Security project demonstrates a capability to provide source and content integrity protection to data-in-transit by employing server-to-server confidentiality protection to data-in-transit by employing server-to-server encryption."

Comment: There exists disagreement regarding the boundaries of data at rest and data in motion. Please see: https://en.wikipedia.org/wiki/Data_at_rest , under heading "Alternative Definition": "There is some disagreement as to the boundary between data at rest and data in use."

- **Page 49, Line 877-879**

4.5.3 ISC (security collaborator contributions)

"BIND[21] is open source software that is considered the reference implementation of DNS, but it is also production-grade software, suitable for use in high-volume and high-reliability applications."

Comment: Consider adding license information about BIND to be consistent with other OSS references in the guide.

Suggested text: BIND versions prior to BIND 9.11.0 are released under the ISC License. (https://www.isc.org/downloads/software-support-policy/isc-license/)

- **Page 112, lines 125-126**

2.1.7 Adding and Removing Network Users

"When a user leaves an organization or access to network resources is revoked for other reasons, it is necessary to revoke the credentials that associate the user with the organization."

Comment: Consider adding, "and it may be in the best interest of the organization to do so as soon as possible, after the user is separated from the organization."

- **Page 116, line 234**

"named-checkzone" at the beginning of a sentence.

Comment: Usage question: Whether "named-checkzone" at the beginning of a sentence should be capitalized.

- **Page 150, lines 45-47**

3.1.1.2 OpenSSL Installation on Mac OS

"Normally, there is no need to install a separate set of cryptographic libraries for Mac OS. OpenSSL is installed in the standard Mac OS distribution provides the same functionality However, if there is a desire to upgrade the standard installation an alternative repository tool…"

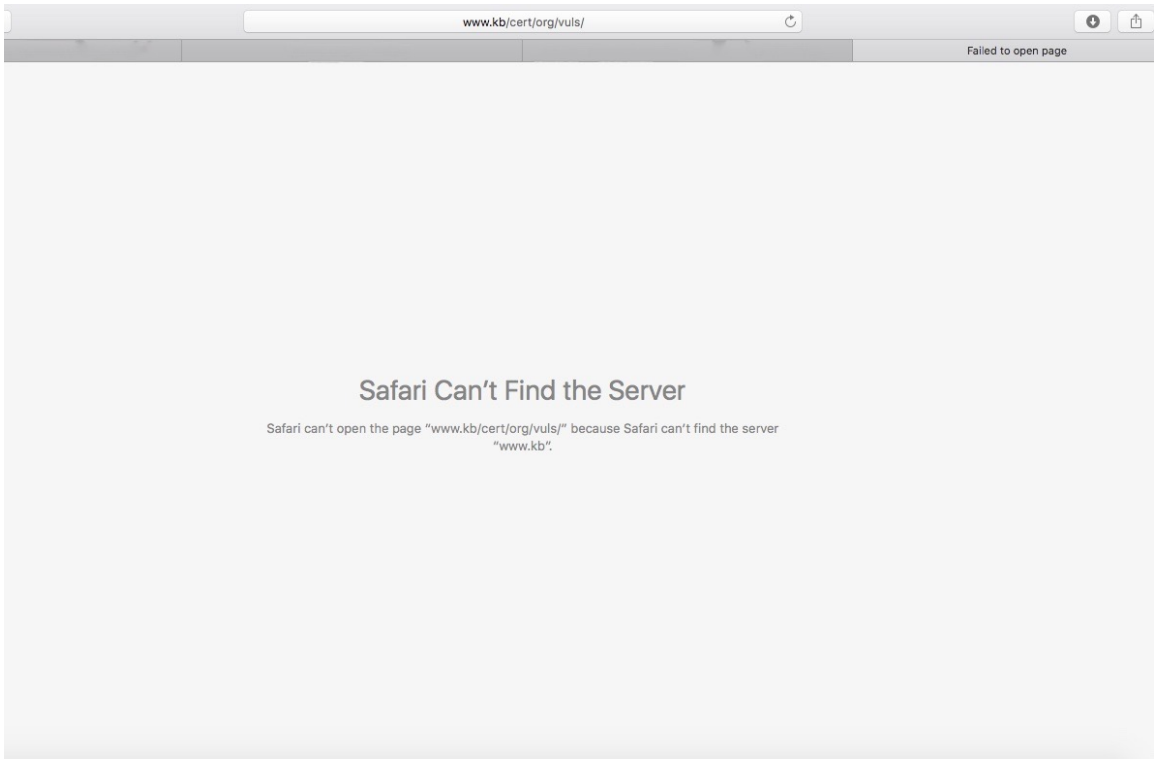
Comment: Usage/grammar. Suggest the following alternate text:

"Normally, there is no need to install a separate set of cryptographic libraries for Mac OS. OpenSSL ~~is~~ if installed in the standard Mac OS distribution, provides the same functionality. However, if there is a desire to upgrade the standard installation an alternative repository tool…"

- **Page 185 line 22**

"Refer to CERT/CC's Vulnerability Notes Database at http://www.kb/cert/org/vuls/"

Comment: Was unable to access this site via Safari on 12/18/2016, approx. 22:38EST. (Pls see screenshot below.)



It is my sincere hope that these comments are helpful; please feel free to reach out with questions or comments.

Kind regards,

Martha C. Chemas, Esq.
244 Fifth Avenue, M223
New York, NY 10001