Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-1108**
Office Instruction Title:	**Web Application Standard**
Revision Number:	**2.0**
Effective Date:	**September 17, 2018**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-1108, “Web Application Standard,” provides descriptions and protection methods for major web application vulnerabilities that must not be present for web applications in the NRC production environment.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	8/23/18
CIO	David Nelson	/RA/	8/28/18
CISO	Jonathan Feibus	/RA/	8/23/18

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-1108

Web Application Standard

1 PURPOSE

CSO-STD-1108, "Web Application Standard," provides the minimum security requirements that must be applied to all Nuclear Regulatory Commission (NRC) web applications in production.

This standard is intended to be used by Information System Security Officers (ISSOs) to secure their web applications, and developers to ensure that web applications are developed with a focus on application security and design. Furthermore, the standard is intended to help ISSOs and other NRC stakeholders select and procure secure web applications.

2 GENERAL REQUIREMENTS

This section addresses the general requirements that all ISSOs and web application developers, who are authorized to administer the web applications, or develop software for NRC web application deployment, must comply with as the minimum set of controls. Furthermore, web applications and those involved with software development must follow applicable application security controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (as amended), "Security and Privacy Controls for Federal Information Systems and Organizations," such as Systems and Services Acquisition (SA)-11, "Developer Security Testing and Evaluation."

The Open Web Application Security Project (OWASP) has published consensus documents covering the following:

- Most prevalent and severe web application security risks,
- Methods to protect against these risks and secure web applications, and
- Information regarding how to test and verify web applications to determine their security risks.

Several OWASP documents are required or recommended for use as specified in this standard to aide in the security of NRC web applications.

All NRC web applications must not be susceptible to any of the latest OWASP Top 10 Application Security Risks. The OWASP Top 10 Application Security Risks is a list compiled by OWASP and is based on vulnerabilities data gathered from hundreds of organizations and over 100,000 real-world applications and application programming interfaces (APIs). Appendix C, OWASP and Other Web Application Security References, lists the latest version of the OWASP Top 10 and associated risks at the time of this standard's publication.

Federal Risk and Authorization Management Program (FedRAMP) authorized cloud services providing low-code or no-code web application development platforms must comply with all

requirements stated in this standard that are under the control of and can be configured/specified by NRC privileged users with access to the service (e.g., system administrators).

3 SPECIFIC REQUIREMENTS

This section provides specific security requirements that must be adhered to in all web applications deployed at NRC.

3.1 OWASP Top 10 Proactive Controls

For web applications where NRC has the ability to customize code (whether all or in part), the web application must employ the latest version of the OWASP Top 10 Proactive Controls.

Appendix C lists the latest OWASP Top 10 Proactive Controls at the time of this standard's publication.

3.2 External Standards for COTS and GOTS

OCIO is responsible for identifying security configuration standards to be used in the protection of any information system that stores, transmits/receives, or processes NRC information. For Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) web applications (e.g., Microsoft SharePoint, Microsoft Outlook Web Access), where NRC does not have the ability to customize code, the effective NRC security configuration standard (e.g., Defense Information Systems Agency [DISA] Security Technical Implementation Guide [STIG], Center for Internet Security [CIS] Benchmark) is specified by the NRC Computer Security Organization (CSO).

The CSO standards website[1] specifies the security configuration standards that apply for several common COTS/GOTS web applications and security configuration standard and the standards that apply when one is not explicitly listed.

3.3 Web Application Security Testing and Verification

OWASP has published the OWASP Testing Guide for testing the software during the software development lifecycle by the web application developers. This document provides the OWASP

[1] CSO standards website – Specifies and provides the security configuration standards to be followed for several common web applications:
http://fusion.nrc.gov/OCIO/team/CSO/CSO_FISMA_Repository/Forms/AllItems.aspx?RootFolder=%2FOCIO%2Fteam%2FCSO%2FCSO%5FFISMA%5FRepository%2FCybersecurity%5FIssuances%2F01%5FSTANDARDS

Security Program Update for Standards – Specifies how security configuration standards are identified when they are not explicitly listed on the CSO standards website:
http://fusion.nrc.gov/OCIO/team/CSO/CSO_FISMA_Repository/Cybersecurity_Issuances/00_CISO_Approved_Informal_Direction/03_Standards.docx

Testing Framework and explains its techniques and tasks in relation to the various phases of the software development lifecycle.

Additionally, the OWASP Application Security Verification Standard (ASVS) provides detailed information regarding how to verify the security of web applications developed for web application security verification and provides software developers with a list of requirements for secure web applications.

NRC ISSOs, web application developers, and security assessors must use the Chief Information Security Officer (CISO) authorized Web Application Security Testing/Assessment Tools as specified in Appendix C. Additionally, the latest OWASP Testing Guide and ASVS documents should be used to assist in testing and security verification of the NRC web applications during the software development cycle and in deployment.

APPENDIX A. ACRONYMS

API	Application Programming Interface
ASVS	Application Security Verification Standard
CIS	Center for Internet Security
CISO	Chief Information Security Officer
COTS	Commercial Off-the-Shelf
CSO	Computer Security Organization
DISA	Defense Information Systems Agency
DoS	Denial of Service
GOTS	Government Off-the-Shelf
FedRAMP	Federal Risk and Authorization Management Program
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OWASP	Open Web Application Security Project
SA	Systems and Services Acquisition
SP	Special Publication
SSRF	Server-side Request Forgery
STIG	Security Technical Implementation Guide
XML	Extensible Markup Language
XSS	Cross-Site Scripting
XXE	XML External Entity

APPENDIX B. GLOSSARY

Application Developer	A computer professional whose primary role involves developing and/or implementing software applications.
Commercial Off-the-Shelf	Software products developed by commercial organizations for the general public.
Cross-Site Scripting	Refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application.
Government Off-the-Shelf	Software products (available for use by Government Agencies) that are developed by the NRC or another U.S. Federal, State, Local, or Tribal Government Agency.
Low-Code or No-Code Web Application Development Platform	Development platforms used for application software development through graphical user interface and configuration instead of the traditional use of computer programming. A low-code platform allows developers to create web applications using point-and-click and drag-and-drop and metadata model methodology.
Open Web Application Security Project	An open-source application security project that is managed and supported by the OWASP Foundation, which is a non-profit organization that focuses on improving the security of application software.
OWASP Top 10	Identifies the most critical web application vulnerabilities that face organizations today.
Web Application	An application that is accessed using a web browser over a network, such as the internet or the NRC intranet. Static file listings on a web server are not considered web applications.
XML External Entity	A specific type of Server-side Request Forgery (SSRF) attack, whereby an attacker is able to cause Denial of Service (DoS) and access local or remote files and services, by abusing a rarely used feature in XML parsers.

APPENDIX C. OWASP AND OTHER WEB APPLICATION SECURITY REFERENCES

OWASP Top 10 Application Security Risks

The Top 10 Application Security Risks for 2017 consists of:

- A1:2017 Injection
- A2:2017 Broken Authentication
- A3:2017 Sensitive Data Exposure
- A4:2017 Extensible Markup Language (XML) External Entity (XXE)
- A5:2017 Broken Access Control
- A6:2017 Security Misconfiguration
- A7:2017 Cross-Site Scripting (XSS)
- A8:2017 Insecure Deserialization
- A9:2017 Using Components with Known Vulnerabilities
- A10:2017 Insufficient Logging & Monitoring

These risks are selected and prioritized according to the prevalence data, in combination with consensus estimates of exploitability, detectability, and impact.

The Top Ten List of vulnerabilities are captured in detail, with mitigation strategies, in the OWASP Top 10 2017 Web Application Security Risks at:
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

OWASP Top 10 Proactive Controls 2016, v2.0

The proactive controls specified in this version include the following:

1. Verify for Security Early and Often
2. Parameterize Queries
3. Encode Data
4. Validate All Inputs
5. Implement Identity and Authentication Controls
6. Implement Appropriate Access Controls
7. Protect Data
8. Implement Logging and Intrusion Detection
9. Leverage Security Frameworks and Libraries
10. Error and Exception Handling

All NRC web application developers should utilize proactive controls specified in OWASP Proactive Controls 2016 v2.0. Implementation details for these controls are provided in OWASP Proactive Controls 2016 v2.0 at:
https://www.owasp.org/images/9/9b/OWASP_Top_10_Proactive_Controls_V2.pdf

Web Application Security Testing and Verification

At the time of the publication of this standard, Veracode is the testing tool authorized by CISO for performing web application security testing and is used to perform static application security testing. All web applications with any customized code must be assessed using Veracode as specified in the below Cybersecurity Program Update for Authorization and Continuous Monitoring Guidance:
http://fusion.nrc.gov/OCIO/team/CSO/CSO_FISMA_Repository/Cybersecurity_Issuances/00_CISO_Approved_Informal_Direction/05_Authorization%20and%20Cont.%20Mon.%20Guidance.docx

The NRC enterprise point-of-contact with Veracode is provided in the above referenced guidance document and can be consulted for information related to Veracode use.

Please note that additional testing tools and application-specific testing scenarios are defined in the OWASP Testing Guide and ASVS, which can be utilized as appropriate (in addition to the required use of Veracode). The latest versions at the time of the publication of this standard can be found at:

- OWASP Testing Guide, v4.0: https://www.owasp.org/images/1/19/OTGv4.pdf
- OWASP ASVS, v3.0.1: https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

CSO-STD-1108 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
8-Aug-12	1.0	Initial Release	CSO web page and notification of ISSO forum	Upon request
21-Aug-18	2.0	Updates with latest requirements	OCIO/CSO web page	Upon Request
7-Jan-19	2.0	Errata changes for document identifier and organizational changes.	Post to OCIO/CSO web page.	N/A