# Open Web Application Security Project (OWASP)

# Draft NIST SP 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

## Response

This response is submitted on behalf of the Open Web Application Security Project (OWASP). The response includes explanations and suggested changes.

### 3.2.5 Access to an Location of the PII

**Explanation** Many organisations are now using web technologies to deliver functional applications. Teleworkers may access web-enabled systems directly and this means that PII is stored in, and transferred from, many more locations including systems hosted by third parties, network devices and user's own computers.

**Suggested change** Amend the sentence which ends "Another element is the scope of access to the PII, such as whether the PII needs to be accessed from teleworkers' systems and other systems outside the direct control of the organization." to "Another element is the scope of access to the PII, such as whether the PII needs to be STORED ON OR accessed from teleworkers' systems and other systems SUCH AS WEB APPLICATIONS outside the direct control of the organization."

### 3.3.3 Example 3: Fraud, Waste, and Abuse Reporting Application

**Explanation** The example states that the data is collected using a web-enabled system. Therefore the database is not just "accessed by a few people who investigate fraud, waste..." - the web site is publicly available, and submissions are written to the (web) database online. There is a potential here for such information to be divulged to unauthorized users while stored in the online database or in transmission through the existence of security weaknesses that can be exploited. Even internally, the intention might be that only a few people access the database, but that may not be the case.

**Suggested change** In the section "Access to and location of the PII: The database is only accessed by a few people who investigate fraud, waste, and abuse claims. All access to the database occurs only from the organization's own systems.", change this to be "Access to and location of the PII: THE DATA EXISTS ON A SERVER OUTSIDE THE ORGANIZATION'S NETWORK (THE ONLINE SYSTEM) AND ANY VULNERABILITIES IN THE ONLINE WEB APPLICATION COULD LEAD TO A BREACH OF THE PII. ONCE TRANSFERRED INTERNALLY, the database is only MEANT TO BE accessed by a few

people who investigate fraud, waste, and abuse claims - only from the organization's own systems.".

## 4.3 Security Controls

**Explanation** An area where "greater protections" is typically required is in web-enabled applications. OWASP is leading the way in the development of open guides, tools and standards for web application security verification.

**Suggested change** At the end of the first paragraph (before the bulleted items) add, "SEE THE OPEN WEB APPLICATION SECURITY PROJECT APPLICATION SECURITY VERIFICATION STANDARD (ASVS) FOR ONLINE WEB SYSTEM SECURITY CONTROL VERIFICATION.". (footnote link http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)

## Appendix A, Scenario 2: Protecting Survey Data

**Explanation** This scenario concerns an email with a hyperlink to an online survey. The user's data must not compromised while they are entering the data into the application. It is also important that the PII data collected needs to be protected while it is stored on the web-enabled systems.

**Suggested change** In the "additional questions for the scenario", add a new item between items 2 and 3 "HOW ARE THE DATA ELEMENTS COLLECTED, STORED AND USED SECURELY IN THE ONLINE SYSTEMS".

# About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a U.S. recognized 501(c)(3) not-for-profit charitable organization, that ensures the ongoing availability and support for our work at OWASP.

Further information:

- OWASP Foundation
  http://www.owasp.org/index.php/OWASP_Foundation
- About The Open Web Application Security Project
  http://www.owasp.org/index.php/OWASP_Foundation
- The Open Web Application Security Project
  http://www.owasp.org/