

# **OWASP Global Industry Committee**

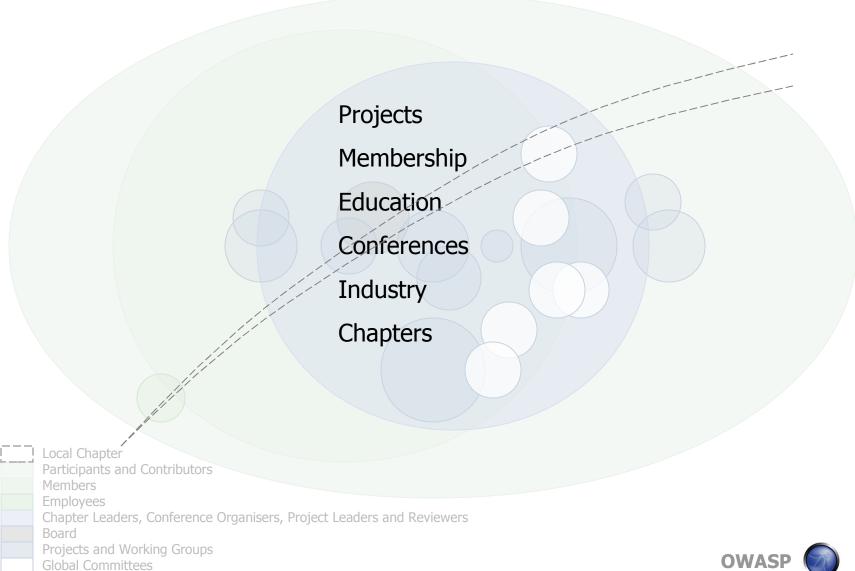


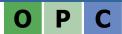
Colin Watson
Global Industry Committee
Member
colin.watson@owasp.org

Copyright © The OWASP Foundation Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

# The OWASP Foundation <a href="http://www.owasp.org">http://www.owasp.org</a>

#### The World of OWASP





## **Industry Committee**

- Rex Booth
- David Campbell
- Georg Hess
- Eoin Keary
- Colin Watson
- Tom Brennan
- Outreach
- P Position paper / response
- Collaborate with other organisations

#### **InfraGard**

- Collaboration between the US FBI and maintainers of critical national infrastructure
- Presentation to Denver chapter of InfraGard
- Completed December 2008 and most basic level most basic level between the Federal Bureau of between the Federal Bureau of state and local between the Sector InfraGard is an association of the sector In









#### **DPC BS 8878:2009**

Draft for Public Comi

- Draft British Standard
- First official response
- "The goal of any web project should be to create web experiences that are accessible, usable and enjoyable for everyone."

Standards Which implement International or European publications referred to in this

- Safe and secure?
- Response submitted 31 January 2009 Information on the co-operating organizations represented on the committees referenced above may be obtained from the responsible committee secretary. Further copies of this draft may be purchased from BSI Custom

available from BSI Customer Services.



# **Digital Britain Interim Report**

- A vision for Britain's digital economy
- "Empowered and informed consumers and citizens fully equipped to take advantage of the opportunities convergence brings."
- "Internet: looking at a range of issues affecting internet users, such as user security and safety and a workable approach to promoting content standards."

Technology and Broadcasting By Command of Her Majesh

■ Response submitted 11 March 2009

#### **Draft NIST SP 800-122**

- Document to assist US Federal agencies in protecting the confidentiality of Personally Identifiable Information (PII)
- Added information and corrections to online related examples
- Response submission due 13 March 2009



#### **Draft NIST SP 800-53 Revision 3**

- Key information security document for US federal sector
- Controls to comply with the Federal Information Security Management Act (FISMA)
- First major update since 2005
- In progress



#### **Consensus Audit Guidelines**

- Prioritized baseline of information security measures and controls
- Subset of NIST SP 800-53 Rev 3 Controls
- 20 controls (categories) including "Application ainst cyber attacks has become one of the Nation's highest priorities. To achi Securing our Nation against cyber attacks has become one of the Nation's highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must defense must be this objective, networks, systems, and the operations teams that are successful defenses must be against external attacks. Furthermore, for those external attacks that are successful. Software Security" this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. Furthermore, for those external attacks that are successful, defenses must against external attacks. Furthermore, for those external attacks on internal networks as attacks against external attacks. Furthermore, for those external attacks on internal networks against external attacks. against external attacks. Furthermore, for those external attacks that are successful, defenses must be capable of thwarling, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

Government Affairs Committee moved to make this same tenet central to the Federal Information Security

Management Act in drafting FISMA 2008. That new proposed legislation calls upon Federal agencies to

we that testing is up to date and comparable, by agreeing on common

"Establish security control testing protocols that ensure that the information "Establish security control testing protocols that ensure that the information on infrastructure of the agency, including contractor information systems operations attacks in the infrastructure of the agency, including contracted against known wilnershill the agency are effectively protected against known wilnershill the agency. ingrastructure of the agency, including contractor information systems operating on attacks, and behalf of the agency, are effectively protected against known vulnerabilities, attacks, behalf of the agency, are effectively protected against known vulnerabilities.

■ In progress A central tenet of the US Comprehensive National Cybersecurity Initiative (CNCI) is that "offense must inform defense" In other words knowledge of actual attacks that have comprehensive described and attacks that have comprehensed and attacks that have comprehensed and attacks that have comprehensed attacks the have A central tenet of the US Comprehensive National Cybersecurity Initiative (CNCI) is that "offense must inform defense". In other words, knowledge of actual attacks that have compromised Homeland Security as the Essential foundation on which to construct effective defenses. mrorm defense". In other words, knowledge of actual attacks that have compromised systems provides and the essential foundation on which to construct effective defenses. The US Senate Homeland Security the essential foundation on which to construct effective defenses. The US Senate Homeland Security defenses. The US Senate Homeland Security and the essential foundation on which to construct effective defenses. the essential foundation on which to construct effective defenses. The US Senate Homeland Security and Government Affairs Committee moved to make this same tenet central to the Federal non-Federal agencies to Management Affairs Committee moved to make this same tenet central to the Federal agencies to Management Affairs Committee moved to make this same tenet central to the Federal agencies to Management Affairs Committee moved to make this same tenet central to the Federal Region Figure 1997.

spread inside a compromised network.



#### **DPC BS 10012**

- Implementation of a Personal Information Management System (PIMS)
- PI rather than information security (IS)

Annex A (informative) The Plan-Do-Check-Act (PDCA) cycle

• 1 - PDCA cycle applied to the management of personal information

esiplify | Coblight | Data Frotection

■ In progress Specification for the management of persona

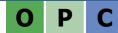




# **OWASP Intrinsic Security Working Group**

- "Act as a consumer awareness group for web application frameworks security mechanisms and browser security features"
- Letter consultation and mailing on browser security issues of HTTPOnly, disabling of "autocomplete" features within cross-domain iframes and implementation of "jail" tags





#### **Contribute**

- Participate in OWASP projects
- Suggest organisations to engage with and documents/standards/drafts to comment on
- Provide input to the response creation and review process
- Join the Global Industry Committee's mailing list

http://www.owasp.org/index.php/Global\_Industry\_Committee

## **End**