



# **OWASP**

## **Global Industry Committee**

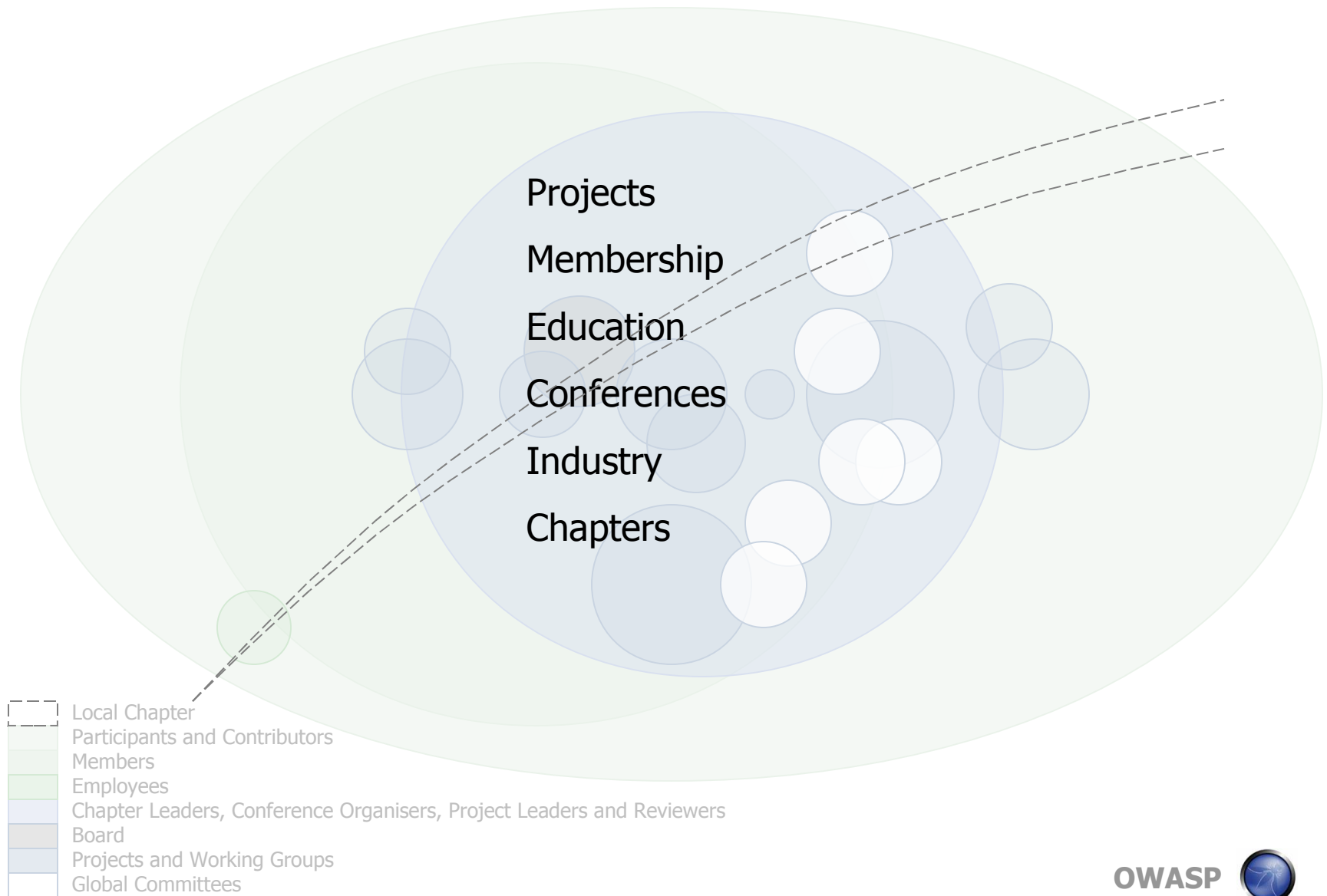
**Colin Watson**  
**Global Industry Committee**  
**Member**  
colin.watson@owasp.org

**OWASP**

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**  
<http://www.owasp.org>

# The World of OWASP

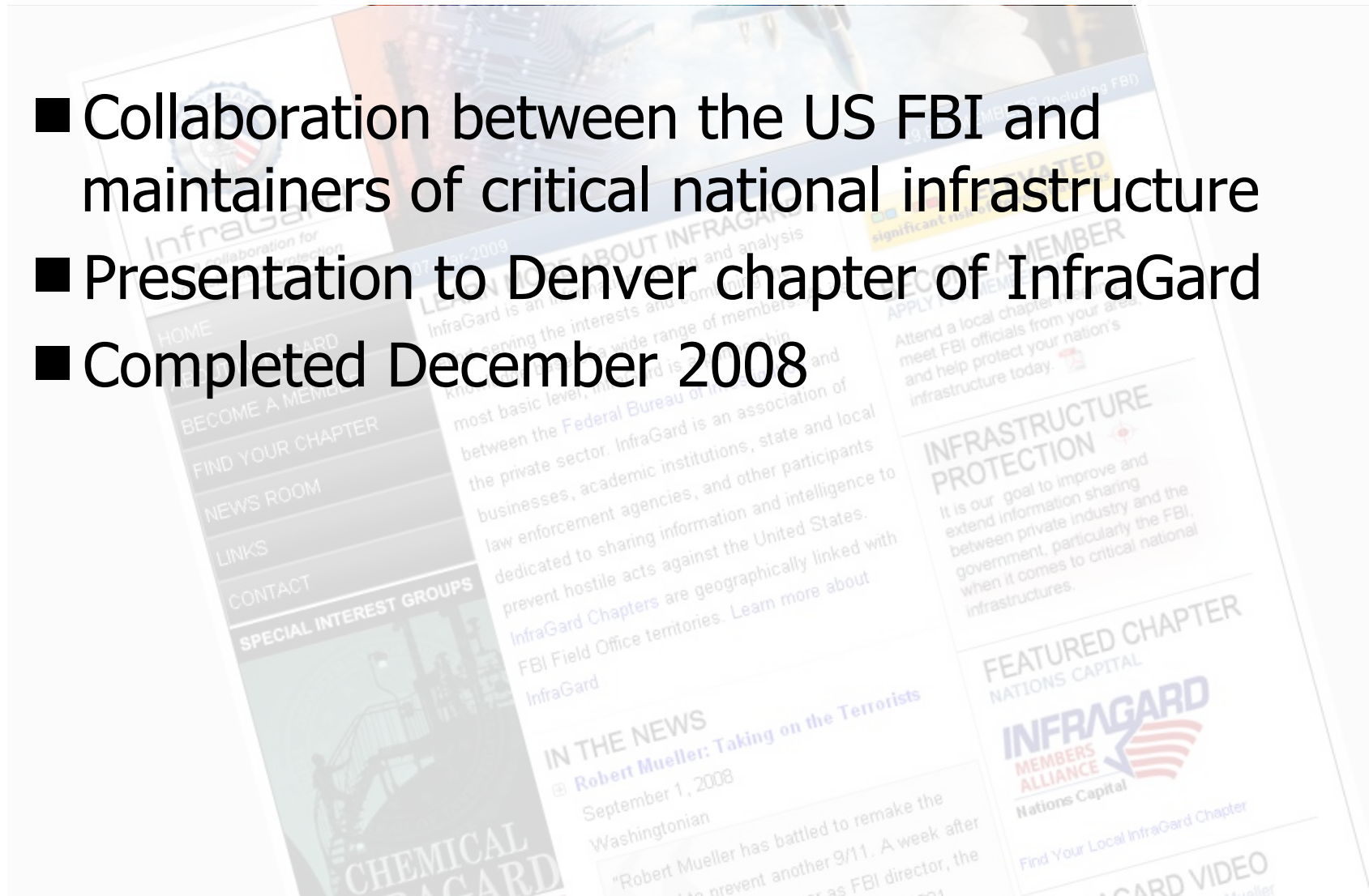


# Industry Committee

- Rex Booth
- David Campbell
- Georg Hess
- Eoin Keary
- Colin Watson
- Tom Brennan
  
- O** Outreach
- P** Position paper / response
- C** 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



# DPC BS 8878:2009

- 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."
- Safe and secure?
- Response submitted 31 January 2009



# 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."
- Response submitted 11 March 2009

Presented to Parliament by  
The Secretary of State for Culture, Media and Sport  
and the Minister for Communications,  
Technology and Broadcasting,  
By Command of Her Majesty



# 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

Special Publication 800-122  
(Draft)

NIST  
National Institute of Standards and Technology  
Department of Commerce

Guidelines for Protecting Personally Identifiable Information (PII)  
(Draft)

Recommendations of the National Institute  
of Standards and Technology

Erika McCallister  
Tim Grance  
Karen Scarfone



# 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

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

February 2009



U.S. Department of Commerce  
Otto J. Woff, Acting Secretary  
National Institute of Standards and Technology  
G. Gallagher, Deputy Director





# 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 Software Security"
- In progress



# DPC BS 10012

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



# 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](http://www.owasp.org/index.php/Global_Industry_Committee)

# End