The OWASP Application Security Code of Conduct for Government Bodies

(The OWASP "Green Book")

Version 1.11 (10th September 2011) Draft

Introduction

Government Bodies (national, regional and local government, departments, directorates, agencies and other types of statutory body) are massive consumers of application technology, and also have influence over the operation of many industries and the behavior of individuals. We believe that Government Bodies should use this power to ensure that software applications are secure enough for their intended purposes. We offer this code of conduct to help guide Government Bodies to improve the state of application security in their own applications and all those under their jurisdiction.

Code of Conduct

1. **The Government Body MUST establish and enforce a standard that requires application security for organizations and applications under their jurisdiction.**

   Given the rapid influence of application technology over all aspects of modern life, virtually every government body is now responsible for some aspect of application security. We ask you to establish a standard that captures your requirements for protecting data, ensuring safety, defending citizens, etc… We do not specify the exact form or substance of this standard, only that it represent your desire for applications that affect your jurisdiction to be secure.

2. **The Government Body MUST build application security into software acquisition guidelines.**

   One of the most powerful forces in the information technology industry is the buying power of governments worldwide. As a massive consumer of application technology, we believe that including appropriate language in acquisition guidelines will strongly encourage the software industry to do a better job with application security. We do not suggest what this language should contain, but point to our Software Security Contract Annex[i] as a possible starting point.

3. **The Government Body MUST provide OWASP a "notice and comment" period when releasing laws and regulations that are relevant to application security.**

   OWASP wants to help government bodes create laws and regulations that will result in improvements in application security. Ideally, we would be involved from the beginning in the creating of the laws regulations and guidance, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

4. **The Government Body MUST define or adopt a definition of application security.**

   Without a definition of application security, government bodies may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all bodies. Rather, we simply suggest that government bodies must have such a definition in place. We recommend using OWASP materials as a way to help figure out what that definition should encompass.

5. **The Government Body MUST create and promote public service messages focused on application security.**

   By creating and promoting a public service message that focuses on application security, government bodies demonstrate the importance of this issue in a simple and direct way. We do

not attempt to specify the exact form or substance of the message, simply that it should encourage all organizations and individuals to understand the risks and take appropriate action.

Recommendations

A. The Government Body <u>SHOULD</u> be an OWASP Supporter.

The main benefit of becoming an OWASP Supporter[ii] is to demonstrate your belief that application security is important and that you are working to build a robust information-age economy and providing a suitably skilled workforce that attracts investment.

B. The Government Body <u>SHOULD</u> assign a liaison to OWASP.

OWASP has a group that focuses on improving application security in government bodies. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The body can define their level of participation.

C. The Government Body <u>SHOULD</u> encourage educational institutions to focus on application security.

We believe that educational institutions represent a unique opportunity to influence software developers and other information technology students while they are still forming their ideas, ethics, and values. Government bodies can influence these organizations to focus on application security and hopefully get their institution in line with the OWASP Code of Conduct for Educational Institutions ("The OWASP Blue Book")[iii]. Government bodies might take the opportunity to sponsor training in application security for educational institutions.

D. The Government Body <u>SHOULD</u> leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer government bodies. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, eLearning, and educational materials that are available for government bodies to use and modify free of charge. Government bodies are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

References

i. Software Security Contract Annex, OWASP
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

ii. Membership, OWASP
https://www.owasp.org/index.php/Membership

iii. OWASP Code of Conduct for Educational Institutions ("The OWASP Blue Book")
https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#tab=Educational_Institutions

OWASP Application Security Codes of Conduct

In order to achieve our mission, OWASP needs to take advantage of every opportunity to affect software development everywhere. At the OWASP Summit 2011 in Portugal, the idea was created to try to influence educational institutions, government bodies, standards groups, trade organizations and groups active in the application security space. We set out to define a set of minimal requirements for these organizations specifying what we believe to be the most effective ways to support our mission. We call these requirements a "code of conduct" to imply that these are normative standards, they represent a minimum baseline, and that they are not difficult to achieve.

Government Bodies wishing to announce their compliance with this Code of Conduct should read the associated information on statements of compliance:

https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#compliance

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and all the participants in the working sessions on Outreach to Educational Institutions, and Minimal AppSec Program for Universities, Governments and Standards Bodies at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The latest version of this document, and the other Codes of Conduct, can be found at:

https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

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 true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

https://www.owasp.org