HOST Project Funding Application
Introduction

Georgia Tech Research Institute (GTRI), through funding by the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T), Cyber Security Division is responsible for carrying out key components of the Homeland Open Security Technology program (HOST).

The HOST program was created to identify new, emerging and undervalued open source solutions to cyber security challenges and to share that information broadly; to make strategic investments in projects with high-impact potential; to encourage innovation by enabling cross-industry collaboration. The Investment component of the program is intended to contribute seed investment in advanced research and development activities that support national cybersecurity objectives and have the potential to create sustainable project communities.

The Investment program is seeking funding applications for projects which fall within its mission.

General Guidance

As a general rule, any effort that contributes to an open source approach to cybersecurity will be considered. Ideal applications would include projects which are:

- Open source (either code or content)
- Built upon existing open source work or projects already underway
- Affiliated with an organization or community that can sustain the effort after the funding is expended

Reference projects: Recent program investments have included contributions to the development of Intrusion Detection Systems (IDS) and government certification of open source security standards. Other projects now under consideration include piloting deployment of OSS security systems in a municipal government environment; development and publication of guides to best security practices for web applications.

Case Study

All funded projects will participate in pre- and post-project surveys and a case study for the purpose of information sharing.

For additional information please email your inquiry to investments@opencybersecurity.org

HOST Investment Funding Questionnaire
Required Proposal Components

Please describe your project in narrative form using clear, simple prose. The topic statements listed under each section are required. You may include additional information as desired.

1 – Sponsoring Organization

- Formal Project Name: **OWASP OpenSAMM Reboot Project**
- Name of sponsoring organization: **OWASP Foundation**
- Primary contact at sponsoring organization: **Samantha Groves**
- Email address for primary contact: **Samantha.Groves@owasp.org**
- Phone of primary contact: **480-800-9830**
- Mailing address of primary contact:

  1200-C Agora Drive, #232
  Bel Air, MD 21014
  United States of America

2 – Project Summary

In 200-400 words, please write a summary of your project.

Include the amount of funding requested, the proposed start date and the estimated months required to complete the project.

The OWASP Foundation proposes to initiate the OWASP OpenSAMM Reboot Project. The original OWASP Software Assurance Maturity Model (SAMM) is an open framework that helps organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM can aid in the evaluation of an organization's existing software security practices, building a balanced software security program, demonstrating concrete improvements to a security assurance program, and defining and measuring security-related activities within an organization. This project was first developed in the past through volunteer contributions, and has continued to be updated regularly by the OWASP community since its inception. OpenSAMM is one of OWASP's most widely used and distributed projects, and it is currently in a position where it needs to be updated, re-vamped, and re-promoted.

This year, the OWASP Foundation made the decision to assist the project with funding support to aid in the re-design and re-development of OpenSAMM, which is why the OWASP OpenSAMM Reboot Project was created. The OWASP led, reboot initiative will focus on gathering key players in the application security and development communities to design, develop, and distribute two new version of the OpenSAMM Framework. Moreover, this reboot initiative will aid in the development of an online web application that will facilitate the use of the framework.

The funding is needed as the original OWASP OpenSAMM Project has simply reached a point where a more dedicated team is needed to complete the work required to create an updated, high quality framework with training material. The amount requested is $121,000 USD. The project would begin immediately after receiving funds, and we estimate that the time to completion will be 2 years.

3 – Problem Statement

In 250-750 words, please describe the problem(s) this project will address:

Describe in detail the high-level security problem this project is intended to address. Please explain technical concepts and terms in both a technical and nontechnical manner so that non-technical readers may understand the concepts presented.

Building secure software is a difficult problem. The complexity of modern applications and the technology used to build these, advance in a fast pace. Overall, it is well known how to technically build secure applications, yet in most cases, projects and organizations fail to deliver this (and statistics show that the situation is not really improving ...). This is due to a combination of factors that are far beyond technical knowledge, and are more related to the organization's view towards software quality and security assurance. Security is a brittle property of software, and many different enterprise-related elements must be implemented and aligned to make this happen.

OpenSAMM, in its first version (V1, 2009), was defined in an era where there was little global understanding of and consensus on how to build secure applications beyond the purely technical level. It originated out of process models such as Microsoft SDL, OWASP CLASP and TouchPoints (to name a few), of which the common feeling was that these were necessary, but not sufficient to this end. OpenSAMM (as well as other models such as BSIMM) can, in that respect, be considered to further maturation of these process models. Yet, OpenSAMM takes a different perspective by taking the philosophy and the structure of a maturity model and building upon it (similar to CMM, but specifically aimed at building secure software). These models are also referred to as software assurance models. The definition of OpenSAMM has been an important milestone in the quest for building secure software that has been an inspiration for many community activities, as well as the foundation of similar models.

In this project, we would like to tackle a number of problems that exist with the current model.

Firstly, the current model is four years old. While it has proven to be a balanced and solid model, experience and new insights have taught us that there is room for very specific improvements. For instance, the rating model does not work flawlessly under all circumstances, nor does it have support for agile development methods. These could be significantly improved.

Secondly, there is a lack of empirical data. After all, most organizations do not want to be the best in class, they rather want to be as good as average (or just a bit better); they certainly do not want to be the worst in class. In order for organizations to make this evaluation, empirical data is necessary. The gathering of this data is based on manual analysis, and must take into account a lot of factors. We consider two complementary strategies to get to this data: asking companies for their data (potentially using specific incentives) and doing analysis of organizations ourselves. Models like BSIMM take a different stance and are actually based on such data from organizations based all over the world. This is often said to be the most important competitive advantage of the latter model.

Thirdly, OpenSAMM is a secure development maturity model without any tooling. Supporters and practitioners have been creating tools (questionnaires, graphical models, evaluation sheets, and so forth) in a need-to-have and ad-hoc manner. Some of these tools have been shared (via the OpenSAMM website and blog) and adopted, while others might not even be known to the community. One of the goals of this project is to get to a good tooling base for the OpenSAMM model. This includes an online web application where organizations could get immediate advice on what they should be doing in their organization to improve their software assurance stance.

Finally, different models have co-existed for several years now, but up till now, no standardization efforts have taken place. To this end, we want to reach out to standardization bodies, and try to build towards standardization for software assurance. We currently have contacts with ISO, and we are considering integration with COBIT and other models.

Describe similar efforts that have been made in the past by your organization or other organizations to solve this problem and what results have been achieved. If past projects have failed, please explain why and how this project will be different.

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. OWASP is more than qualified to undertake this project as the organization, and its many industry contributors, have been involved with similar projects that help in securing web applications for more than 11 years. In addition, the OpenSAMM project has already been developed, and has been a very successful project for the Foundation. The OpenSAMM framework has been used by thousands, and OWASP hopes to update the framework in the hopes of continuing to provide value to the software security community.

4 – Solution Statement

In 250-750 words, please describe the solution(s) this project will deliver:

Please describe your solution in detail, in both technical and non-technical terms.

The goal of this project is to advance the OpenSAMM software assurance model in different areas in order to increase further adoption of the model, as well as collaboration between its users. Adoption of the model is influenced by many factors. Currently, we consider the following key factors in model adoption: model improvements, empirical data, tool support, standardization and promotion. As such, the project will focus on these cornerstones. Apart from these, the project will work on building the user community by organizing a number of events to discuss the advancements of the model.

Does your solution involve any technical innovations? If so, please explain what they are and what other innovations could be developed as a result.

OpenSAMM is a secure development framework rather than a technical product. In that sense, the improvements are not of technical nature. The technical aspects of this project will involve the development of a web application that will facilitate the use of the framework.

Please describe, in layman's terms, the scope of the innovations and relative impact.

The core of the innovations in this project is in making the model more usable and accessible to the IT community world-wide. The project starts from an existing model, but is aiming to achieve improvements in supporting tools and usage data. As such, the innovations mainly lie in the development of supporting material for the model, and model improvements. By taking this strategy, the project focuses on some of the most-heard feedback of the project. In that sense, we are convinced that the applicability of the software assurance model will increase, and that these updates will be relevant for most IT based organizations on a global scale.

What social benefit is expected to accrue to cyber security as a result of the solution and how would it accrue based on the scope of the project?

The results produced by this project are free to use and are offered under an open source license. As cyber security is becoming a key issue worldwide, overall qualitative guidance on how to address this problem for software is widely relevant. We expect that people will start looking more and more into secure development or acquisition of software, and models such as OpenSAMM can help enormously in this area.

As this project focuses on improving the applicability of the model, it is clear that the cyber security community in general would benefit from this project. An important point in this area is the standardization activity of the project, which aims at providing a unified model that different types of organizations can turn to. This will aid in aligning and balancing software security efforts overall.

Are the innovations produced by this project contingent upon the successful completion of other related programs or projects? If so, how are they contingent and what are the projects?

This project can be executed in isolation as there are no hard dependencies on other projects to achieve successful results.

5 – Context

In 250-750 words, please describe the context of the problem(s) and solution(s) this project will address:

Describe the technical environment in which the problems exist.

The OpenSAMM model focuses on ensuring the security of software being used within organizations. It is not restrictive as to whether the software has been built or has been purchased; whether the software is a web-based application, a mobile application or any other application. The OpenSAMM model is scalable as it does not matter what type of organization is using the framework (this can range from SMEs to multinationals). Moreover, the framework can be used no matter what methodologies and technologies have been used to construct the application. In that sense, the scope of applicability of the model is extensive.

What is the specific problem or core issue this solution would address?

This project would focus on making the model more applicable. The current model exists as a solid and stable model, yet there's not a lot of supporting material to implement the model in an organization. This project would focus on building the community around the model and to improve tools, empirical data, and standardization of the model in order to increase adoption.

How does the problem or issue relate to your organization and why is your organization qualified to undertake this project?

As mentioned in Section 3, OWASP is an open community dedicated to making software security more visible to both organizations and individuals. We have been advocating the approach of application security as a people, process, and technology problem for 11 years as we feel the most effective approaches to application security include improvements in this area.

Additionally, OWASP is qualified to undertake this project as the organization has been involved with developing and managing similar initiatives for more than a decade. Moreover, OpenSAMM is already an established OWASP project, and has been one of our most popular projects for the past 5 years.

6 – Activities

In 250-750 words, please describe (not just list) the activities of this project:

Connect each step of your work with your goals.

The project consists of a number of complementary activities that will improve the OpenSAMM model and its global adoption. We explain these activities in more detail below.

A first set of activities relates to the building of the OpenSAMM *community*. For this matter, the project will ensure the creation and distribution of quarterly OpenSAMM newsletters, as well as the organization of OpenSAMM workshops at the main OWASP AppSec conferences (USA, Europe, Asia, and Latin America). At the end of the project, a dedicated OpenSAMM summit will be organized to wrap up the project and disseminate the project results.

A second set of activities relates to the gathering of empirical data. Two different approaches will be taken for this milestone. First, we will create two questionnaires to gather specific data. These questionnaires will be sent within the OWASP community and beyond, and limited incentives for completing will be provided. Secondly, we intend to have a project support resource (student, or a professional in sabbatical mode) do a number of case studies of organizations to gather such data in a more proactive manner.

A third set of activities relates to improving the model. Two new versions of the model will be defined (version 1.1 and version 2.0) in which specific improvements will be implemented. Furthermore, we will further work on translating the model into four new languages to facilitate the adoption in non-native English speaking countries.

From an education perspective, we will create training material to allow people to do self-study and/or give presentations on the OpenSAMM model.

To support data gathering and training, an online web application will be created to enable people to do specific analysis of their situation and to get advice on where improvements could be implemented with respect to software assurance in the organization. Such a tool is, to our knowledge, the first in its kind, and it has the potential of supporting a large community.

Finally, a last activity relates to standardization of software assurance. Here, the goal is to work together with standardization bodies such as ISO, NIST, and potentially others to consider creating a common standard for software assurance. Likewise, we will consider linking OpenSAMM to important other standards such as COBIT, ITIL, and so forth.

Describe the specific milestone activities that would be accomplished in this

proposed project.

Each type of activity in the project is different, and we have not planned to have project-wide milestones where everything is aligned planning-wise. Rather, the milestones are simply categorized based on activity. The first milestone, for example, will focus on community and promotion initiatives. The milestone’s activities involve the project summits, the promotion at our AppSec Conferences, and the design and development of our quarterly newsletter. The second Milestone involves the Research and Analysis part of our project. This is where we will develop and send out our surveys to better understand the needs of our consumers, that data of which will be used in our case studies. The third milestone involves the model development and training material development. This is our most important milestone as it involves the design and creation of 2 new versions of the OpenSAMM model, translations as well as development of training materials such videos, manuals and workbooks. The fourth milestone involves the development of an online OpenSAMM web application that aims to facilitate the use of the model in an online setting.

What form of involvement and leadership position will your organization take in this project? Will your organization be donating funds or making any in-kind contributions to help facilitate this project? If so, in what manner and what amount?

The OWASP Foundation will lead this project and provide project management and project support resources to ensure completion and quality control of the OWASP OpenSAMM Reboot Project. OWASP will assist the OpenSAMM Project Leaders with recruitment for volunteers and contributors. Moreover, OWASP will assist with the sourcing of contractors and interns needed for milestone completion. The OWASP Foundation has also donated $700 to the OWASP OpenSAMM Reboot project, and efforts are in place to raise more funds to contribute to this project.

7 – Projected Outcomes

In 250-750 words, please list the concrete, measurable results and specific expected outcomes:

How would you define success for this project?

The value of a framework such as OpenSAMM is proven with the adoption of the model. As such, we consider the project a success when the following conditions are met:

- The OpenSAMM community (creators, users and supporters) increases over the years. During this project, we want to create a more visible and active community.
- The instruments for adopting OpenSAMM are improved, which will make it easier for people to start using OpenSAMM in their organization. Instruments for adoption include

statistical data (for comparison purposes), educative tools and an online OpenSAMM application.

- New versions of OpenSAMM are published during the project. Cybersecurity is an evolving discipline and so should OpenSAMM. We must learn from research and usage and improve the model where we can.

Note that everything being produced during the course of this project will be available free of charge under an open source license.

What measurable outcomes are expected as a result of this project?

The project outcome includes the following measurable results:

- 2 new versions of the model (version 1.1 and version 2.0).
- Data gathered for at least 50 companies.
- Organized at least 5 international OpenSAMM workshops to support the OpenSAMM community.
- Training Materials and a stand alone OpenSAMM web application that will aid in the use of the framework.

How might this project change cyber security within two years? Ten years?

One of the most important contributions of a model such as OpenSAMM is for people to understand what entails the production, acquisition, implementation and support for secure software in an organization. As such, an important improvement will be an improved investment of cybersecurity money and similar return on investment. As such, the overall security posture of software will increase, since people will better understand where to best focus on.

What next steps might follow the completion of the proposed project?

We plan to further develop the tooling based on feedback, e.g. offline version, follow-up of SAMM progress with support for individual teams, and aggregated reporting within an organization. Additionally, we plan on putting together online SAMM metrics/statistics per vertical, and continue to promote SAMM User Group summits. Lastly, we plan to work on the further evolution of SAMM with increased integration of other OWASP projects.

8 – Project Budget

An important component of your proposal is the preparation of an initial high-level budget that is reasonable. Please ensure that everything mentioned in the proposal is accounted for in the budget. Complete every field using your best judgment when projecting project expenses. Provide any detail in the notes section that you feel would be helpful to provide clarity.

If you anticipate support (including in-kind) from an organization other than HOST, please enter those amounts below and use the notes field to describe the nature of the in-kind description.

Budget Definitions

- Personnel - salaries, benefits and associated fringe costs
- Other Direct Expenses - communications/marketing, travel, meeting expenses, project space
- Purchased Services - consultant and/or third-party contractor costs
- Indirect Expenses - administrative expenses related to overall operations Budget Category

HOST	**Support**	**Non-HOST Support**	**Notes**	**Total**
Personnel	$23,000			$23,000
Other Direct Expenses	$28,000	$9,000		$37,000
Purchased Services	$61,000			$61,000
Indirect Expenses				
Grand Total	$112,000	$9,000		**$121,000**

Budget Narrative

Please explain your approach for use of funds if not previously defined in your project approach, activities or other sections of your application; how will funds for personnel be expended, staff or contract work? What services will be purchased? Are these one time expenses, or will the expense require an ongoing commitment to sustain the activity?

The funds will be managed by OWASP staff, and the work done on the project will be used to hire contractors and to fund internship opportunities for students. Services that will be purchased vary but include: design work, software development work, writers, translators, researchers, and video editors. All of these expenses will be one time expenses.

Major Milestone 1: Community & Promotion

- Develop Quarterly newsletter: Online/ DHS *DE*
  Cost: $1,000.00

- Event Promotion: *DE*
  In conference project workshops: $6,000.00/ DHS
  Dedicated Project Summit: $15,000.00/ DHS

- Print & Distribute OpenSAMM book/ DHS
  Cost: $5,000.00 *DE*

- Aligning with Other Standards *Owasp Direct Expense*
  Evaluate Standardisation: $5,000.00 (Man hours/analysis)
  Attend targeted standardisation meeting: $2,000.00
  Attend targeted standardisation meeting: $2,000.00

Stage Total: $36,000

Major Milestone 2: Research & Analysis

- Y1: Create and Distribute first questionnaire
  Cost: $500.00 *P*
  Capture Input: $500.00 *DE*

- Analysis (man hours)
  Cost: $1,000.00: Content *P*
  Publish Results Cost: $500.00: Layout *PS*

- Y2: Create and Distribute second questionnaire
  Cost: $500.00 *P*
  Capture Input: $500.00 *DE*

- Analysis (man hours)
  Cost: $1,000.00 *P*
  Publish Results Cost: Layout $500.00 *PS*

- Case Study Development
  Develop Baseline
  Cost: $2,000.00 P

- Pilot Case Study: $3,000.00 P
- Publish First Results: $2,000.00 PS
- 5 Case Studies: $3,000.00 P
- Analyse Results: $3,000.00 P

- Publish Final Results: $2,000.00: Layout PS

Stage Total: $20,000

Major Milestone 3: Model Development & Training Material Development

- OpenSAMM Release 1: $3,000.00 - Layout and Design PS
- OpenSAMM Release 2: $2,000.00 - Layout and Design PS
- Translations: $4,000.00 PS
- Translations 2.0: $4,000.00 PS

- Education & Training
  Develop Training Videos: $6,000.00 Content intern/contractor P
  Video Editing Videos: $2,000.00 Editing Resource PS

- Education Material: $3,000.00 (ppt. instructor, manuals, workbooks) P
  Publish: $1,000.00 PS

Stage Total: $25,000

Major Milestone 5: Tooling PS

- Sprint 1: $5,000.00
- Sprint 2: $5,000.00
- Sprint 3: $5,000.00
- Sprint 4: $5,000.00
- Final Sprint: $5,000.00
- Deploy: $5,000.00
- Test: $5,000.00
- Production: $5,000.00

Stage Total: $40,000.00

Total Requested by Project: $121,000