# Case for support for the Open Source Technology Improvement Fund

## Introduction.

An unquantifiable privilege that should be shared with all humankind is freedom. How can we ensure that right in an age where governments, criminals, and spy agencies around the world can easily access and control someone's most private information with the click of a button? The Open Source Technology Improvement Fund (OSTIF) believes the ultimate way to ensure freedom to all people is to provide data security for all. We are allowing access to the uncensored internet and giving people control over their digital lives. Our central areas of focus are privacy, security, and agency in a digital world. We are accomplishing this by strengthening free software and educating people on its use. This is the technological response to the digital privacy problem. No matter what surveillance is imposed upon the people, it cannot break the protection of math and science. Through software engineering and powerful encryption we give the world the privacy and, therefore, the freedom it deserves.

## Who Are We?

OSTIF is a corporate (IRS 501(c)3 recognized) non-profit organization that connects free and open security projects with crucial funding and logistical support. These central tenets are driven by public fund-raising and by soliciting donations from corporate and government donors.

OSTIF was created out of its need to exist. Derek Zimmer (Founder, Chief Executive Officer) recognized the opportunity to establish an objective advocate for free and open software. Namely, an advocate that could fill the gap of woefully underfunded and untrusted open-source programs, despite their central role on the internet. Armed with expertise, industry experience, and contacts, Derek reached out to Zach Graves (Vice President of Creative Design) and Amir Montazery (Vice President of Business Development) to create the organization.

## Our Team.

The OSTIF team consists of Derek Zimmer (Founder, CEO), Zach Graves (Vice President - Design), and Amir Montazery (Vice President - Business Development). Each member has their domain to focus on while contributing to the greater objective.

Zimmer has twenty years of experience with internet security, programming, and mathematics and has been involved in the privacy and free information communities for over a decade. He brought Zach and Amir together to create OSTIF based on mutual trust, work ethic and a harmonized vision of how the internet should work in the digital age.

Graves has over five years of teaching experience, enabling us to create effective guide videos, and has a strong design portfolio. He is adept at applying his knowledge in teaching to communicate our message to a less technical audience.

Montazery applies his past experience working for a startup in the San Francisco Bay Area along with his MBA to further develop our business strategy. He brings critical business knowledge in personnel management and professional networking to the team.

## The Problem.

The internet and its users' freedoms have been compromised due to a weak infrastructure that is conducive to mass surveillance, hacking, and censorship. Mass surveillance allows for the weaponization of data collected from users without their consent or knowledge. This data is being leveraged in cyberwarfare campaigns against journalists, political movements, foreign governments, and in many cases against a nation’s own citizens. Right now, people overwhelmingly support keeping the internet open and surveillance-free, regardless of their political affiliations or nationality.

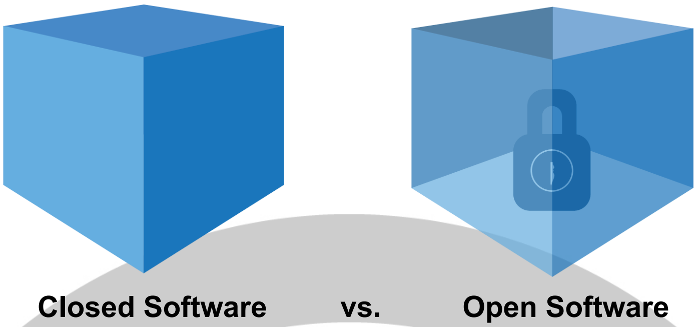
Freedoms that we take for granted, like patient-doctor confidentiality, attorney-client privilege, safe and fair elections, a free press, freedom to organize, and things as simple as having a private conversation with your partner, are in danger of being lost permanently to mass surveillance and organized crime.

The solution lies in free and open software but this software doesn't have the funding to draw the expertise and resources required to make it powerful, trustworthy, verifiable, and easy to use. The resources needed to solve this problem are material, but not available in the current state of the world. Silicon Valley is largely uninterested in privacy because harvesting user data is their business, and giving users easy access to agency over their privacy will damage their revenue streams. This lack of profit motive outweighs the benefit of free, trusted, and secure information for everyone.

## The Solution.

Our solution is to provide the world with powerful free security software that permanently reshapes the internet. This software can be used by everyone in the world to protect themselves from the threats of cybercrime, cyberwarfare, and digital surveillance.

The advantages to open software are verifiability and trust. With traditional closed commercial software you have to trust that things are coded properly and that the application does what it says it does. With open software, you can have experts directly verify that the application meets all security standards and is not compromised by malicious or buggy code.



As an independently funded and objective non-profit, OSTIF seeks out promising free software projects and then reinforces those projects with funding, resources, and expertise to transform the project into a trustworthy world-class cybersecurity app.

This approach gives the world unlimited access to digital privacy for free. Digital security is one of the largest problems facing the modern world, with billions invested into cybersecurity annually, as well as billions more lost in cyber attacks.

This empowers everyone, from an American protecting their banking information, to a Ukrainian journalist who wants to protect their sources on corruption, to an Indonesian farmer with no electricity whose government needs trustworthy security to manage their trade deals, to minorities who fear reprisal from governments for their race or beliefs, to a Chinese citizen who wants access to uncensored world news.

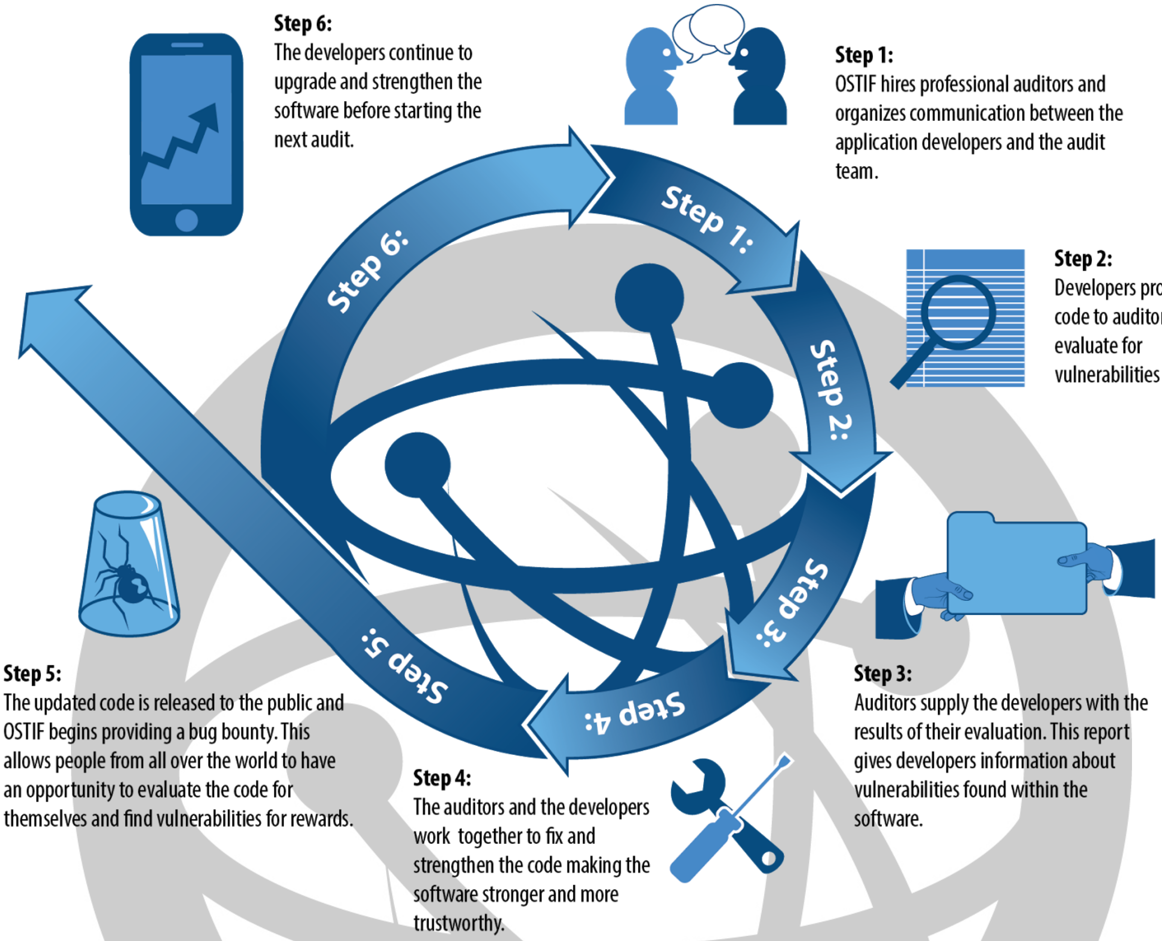
OSTIF’s technological approach is much stronger than a legislative approach because it takes away the ability for bad actors to skirt privacy laws through ignorance or malice. For example, there is no evidence that the American NSA, Britain's GCHQ, or the Russian FSB have changed any of their operations due to EU privacy laws and cybercriminals simply ignore these laws. The technological solution seals the rights of everyone to have access to free information and to be able to protect their own information.

This long-run solution will save society trillions in losses while protecting human rights.

## Our Tactics and Technology.

First, we select a project that meets our criteria for support. The software has to be free of charge, and not under license or copyright that will prevent its free use. It has to solve a major cybersecurity or surveillance problem. It has to be available now and it has to be easy to use.

Once a project is selected, we harden the software with a targeted, efficient, and responsible process.


Step 6:
The developers continue to upgrade and strengthen the software before starting the next audit.
Step 1:
OSTIF hires professional auditors and organizes communication between the application developers and the audit team.
Step 2:
Developers provide code to auditors to evaluate for vulnerabilities
Step 3:
Auditors supply the developers with the results of their evaluation. This report gives developers information about vulnerabilities found within the software.
Step 4:
The auditors and the developers work together to fix and strengthen the code making the software stronger and more trustworthy.
Step 5:
The updated code is released to the public and OSTIF begins providing a bug bounty. This allows people from all over the world to have an opportunity to evaluate the code for themselves and find vulnerabilities for rewards.
Step 6:
Step 1:
Step 2:
Step 3:
Step 4:
Step 5:

1. We look at the app and see if any changes need to be made in order to make the software stronger. We then commission a team to implement those changes.

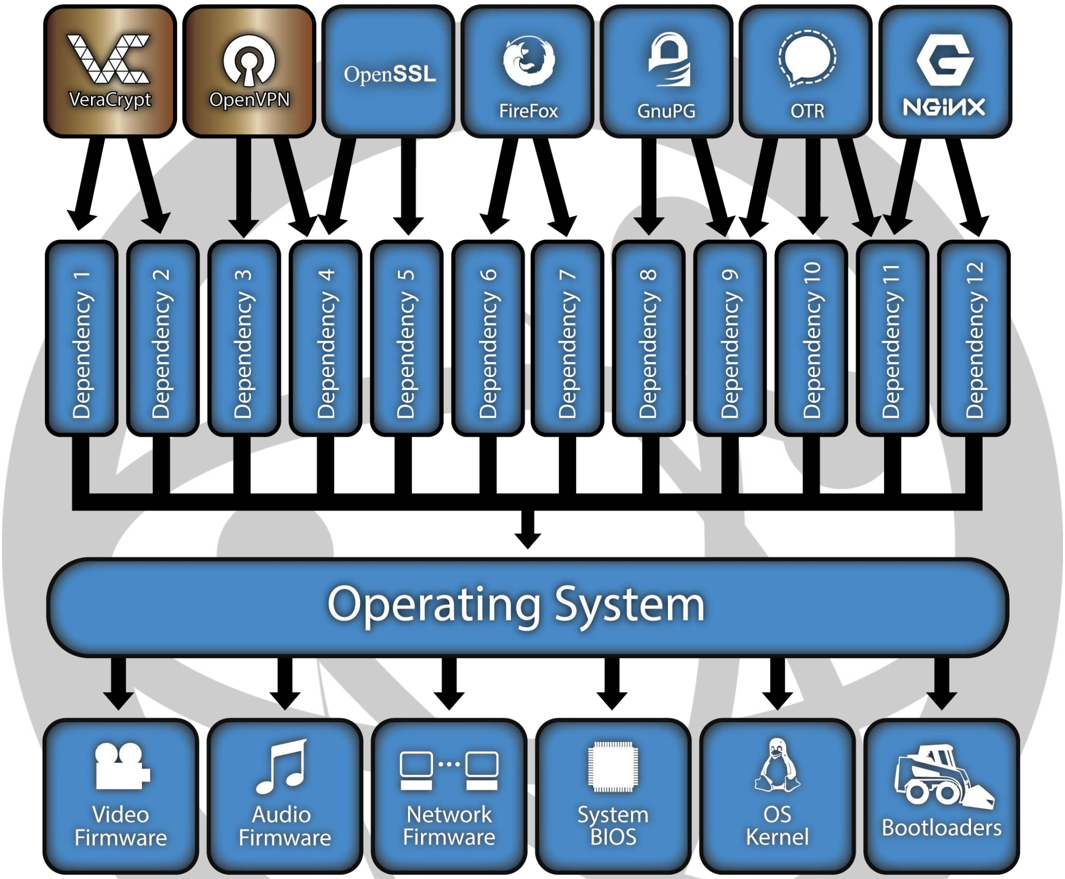
2. We hire a team of security professionals to review all of the code to look for flaws.

3. After the audit is completed and the flaws have been corrected, we create a bug bounty program for the app. The bug bounty is a challenge that anyone can complete in order to receive a cash prize. This allows us to leverage the expertise of the entire world in a cost effective way.
4. If the project has stretch goals for promising new features, we offer grants for research and development of those features.

This process pulls together the resources of the world, both professional and amateur, and creates powerful software for the people of the  world to protect their information.

## Our Long-Term Strategy

Our long-term goals are to systematically improve and certify a full arrangement of safe open-source software, and then work our way down through the dependencies, the operating system, and the hardware to create a complete secure solution that anyone can rely on.



The certification system involves first identifying a single app from each common area of computing, and then going through the improvement process.

**Bronze Certified Software** - A project reaches this tier when it has been audited independently and the bug bounty for the project begins.

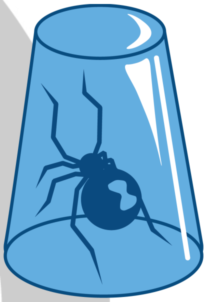
**Silver Certified Software** - A project reaches silver status when it has had an active bug bounty program for six months, and has had no bounty payouts for high or severe bugs for six months.

**Gold Certified Software** - A project reaches gold status after is has conducted research on the needs of its users and is issued a grant from OSTIF to further improve the software to add features or increase usability of the hardened software.

## Evidence of effectiveness.

The process we have defined, which is selecting software, enhancing it to make it easier to use, auditing the code for security flaws, and creating bounties so that anyone in the world can search for and find a bug for a prize, is present in the commercial software world.

Professional auditing is a cornerstone of commercial software. Any respectable software company either sources a company to audit their apps or has a security team on staff that reviews their code. OSTIF brings industry standard professional auditing to free software.



Bug bounties (prizes for amateurs or professionals who find flaws) are present in dozens of commercial projects including apps by Apple, Google, Facebook, American Airlines, and much more (full list at Bugcrowd.com). It has been found to be extremely effective at protecting complex commercial systems from flaws that auditing may have missed. Using the power of the entire world's security experience, and leveraging that knowledge with incentives, leads to impressive results in a cost-effective way!

As for the apps themselves, there is ample evidence of the efficacy of strong encryption. Edward Snowden, has said that "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on." There is also evidence in the Snowden documents that specific applications give the most resourced agency in the world trouble. Three of those applications are in our list of supported apps to be further improved.

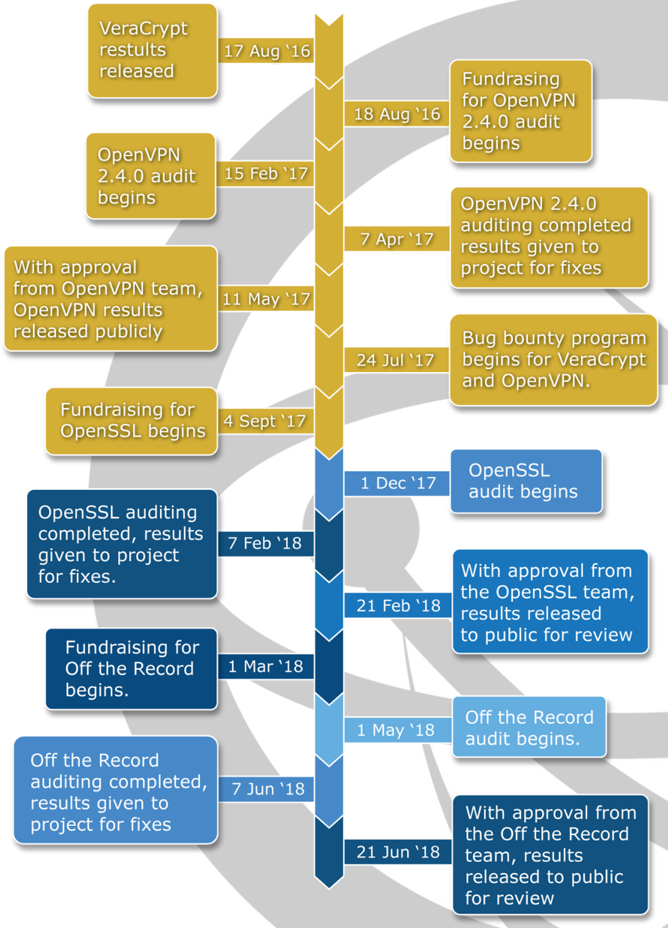
## Previous Track Record of Success.

Our first major accomplishment was our audit of VeraCrypt 1.18. The audit which was conducted by QuarksLab and paid for entirely by our charity found 26 flaws (8 of them critical) in the software that were fully corrected either through code changes or documentation changes to the software that advise special cases in which VeraCrypt should not be used. Because of these efforts, there is now a full disk encryption application that is far more trustworthy and capable of protecting even the most sensitive information. These improvements directly impact the security of the world, and show that we can accomplish all of our goals in a cost-effective way with very little overhead. The results of that audit can be viewed here: https://ostif.org/the-veracrypt-audit-results/

Our second audit was OpenVPN 2.4.0. The audit was conducted by QuarksLab and two critical denial of service vectors were closed, along with five other vulnerabilities. We also created improved documentation for the OpenVPN protocol itself that we passed to the OpenVPN team for free use. This work increased our total number of bugs squashed to 33 after over 1600 man-hours of sponsored security review.

The full results of that audit can be viewed here:
https://ostif.org/the-openvpn-2-4-0-audit-by-ostif-and-quarkslab-results/

## Our Timeline for the Future.



17 Aug '16 VeraCrypt restults released
18 Aug '16 Fundrasing for OpenVPN 2.4.0 audit begins
15 Feb '17 OpenVPN 2.4.0 audit begins
7 Apr '17 OpenVPN 2.4.0 auditing completed results given to project for fixes
11 May '17 With approval from OpenVPN team, OpenVPN results released publicly
24 Jul '17 Bug bounty program begins for VeraCrypt and OpenVPN.
4 Sept '17 Fundraising for OpenSSL begins
1 Dec '17 OpenSSL audit begins
7 Feb '18 OpenSSL auditing completed, results given to project for fixes.
21 Feb '18 With approval from the OpenSSL team, results released to public for review
1 Mar '18 Fundraising for Off the Record begins.
1 May '18 Off the Record audit begins.
7 Jun '18 Off the Record auditing completed, results given to project for fixes
21 Jun '18 With approval from the Off the Record team, results released to public for review

Note: this timeline assumes current levels of funding, changes to this may greatly accelerate the schedules of these programs.

## Our Capacity to Continue Success.

We have built a network of industry partners and individuals who make up our advisory council that spans all areas of the organization's needs from legal to financial to technical. This gives us enormous resources to draw from when we are approaching a new project or idea that the organization wants to undertake.

OSTIF is built from the ground-up to be a low overhead and high performance per dollar operation. We have no central office and conduct all of our business online. We do not engage in expensive marketing. The organization has never and will never take on any debts.

**We have met all of our previous goals and now plan to move forward with OpenSSL 1.1.1 and Off-the-Record messaging.**

## Late 2018:

**In 2018 we plan to expand our adoption of projects as our current supported projects mature. We will be selecting a web server, a database server, a content management system, and an office suite.**

## Our Financial Records.

We have public books, and every dollar that we take in and spend can be tracked through our public books.
https://docs.google.com/spreadsheets/d/1OqWBlNwk5be2c74cRlmYOdhLWPeCjCBAALxYCdMwIaM

We also have released our first annual report, where we achieved our goals of being a 90%+ charity!
https://ostif.org/ostif-financial-report-for-fy2016/

## Charitable Purpose.

This is an enormous problem that faces everyone in the world. The beneficiaries are all of us. Privacy is a fundamental human right that is crucial to free societies and destructive to oppressive regimes. Loss of privacy can lead to discrimination, blackmail, loss of autonomy, and even death. Loss of free information can re-shape your opinions, suppress journalism, spread misinformation, and empower and embolden tyranny. The privacy cause is woven into all of the other causes that make up a free society.

Furthermore, better security provided by free software will dramatically reduce cybercrime and identity theft losses, creating another ancillary benefit to society.

## Why Did Our Team Get Together?

Our team began meeting two years ago to talk about the issues of privacy, surveillance, and censorship. We wanted to do something about it. We wanted to be a force that could change the way the world's citizens engage with one another.

Identity theft has been the number one problem to solve for western economies for decades. Government surveillance is becoming ubiquitous, and the threat of the misuse of that data rises every day that these programs continue to function. The Snowden documents revealed that the world can't fully trust any closed software. As the stakes of cyber warfare and espionage escalate, we can protect ourselves from disaster.

We worked together to find the best approach to fixing this problem for everyone.

We came up with a real and permanent solution, and we are here to change the world.

**We hope that you will join us in creating a safe and equitable digital world for all of us to live in.**

Thank you,

From the Open Source Technology Improvement Fund

Derek Zimmer
Chief Executive Officer
Derek@ostif.org

Amir Montazery
Vice President - Business Development
Amir@ostif.org

Zachary Graves
Vice President - Creative Design
Zach@ostif.org

Visit us at https://ostif.org if you’d like to follow the latest developments!