

Homeland Open Security Technologies



Cyber Security Division 2012 Principal Investigators' Meeting

10/09/11

**Luke Berndt
Program Manager
CyberSecurity Division
Science & Technology Directorate - DHS**

**luke.berndt@dhs.gov
202-254-5332**

What is Open Source?

- OSS: software licensed to users with these freedoms:
 - to run the program for any purpose,
 - to study and modify the program, and
 - to freely redistribute copies of either the original or modified program (without royalties to original author, etc.)
- Original term: “Free software” (confused with no-price)
- Antonyms: proprietary software, closed software
- Not non-commercial; OSS almost always commercial

Myth: OSS always unreliable **Reality:** OSS often very reliable

- Proprietary Unix failure rate: 28%,23%
- OSS: Slackware Linux 9%, GNU utilities 6% [U Wisconsin]

Why is good for Gov?

- Can evaluate in detail, lowering risk
 - Can see if meets needs (security, etc.)
 - Mass peer review typically greatly increases quality/security
 - Aids longevity of records, government transparency
- Can copy at no additional charge (lower TCO)
 - Support may have per-use charges (compete-able)
- Can share development costs with other users
- Can modify for special needs & to counter attacks
 - Even if you're the only one who needs the modification
- *Control own destiny: Freedom from vendor lock-in, vendor abandonment, conflicting vendor goals, etc.*

Why would Gov care?

- \$79.5b IT Budget for Fy12
- 0.7% decrease for Fy13
- \$6.5b for security – 8% of budget
- Industry averages 15-20%

Do more with less and make it secure!

- Increasing security requirements for government
 - Cyberscope, FedRamp
- Unique market, additional requirements
- Little reuse of GOTS solutions
 - Complete redesigns common
 - New contract = new solution

Why might you want to?

- Same list as previous, plus...
- **OSS use:** similar advantages to use of proprietary commercial item
 - Competitive advantage (if uses & others don't), because shared development of item across many users (cost, time, quality, innovation) tends to produce better results
 - Can focus on problem not lower-level issues (if everyone uses)
 - Avoids risks of depending on proprietary commercial items
 - Proprietary third-party: Vendor lock-in risks (costs, abandon,...)
 - A contractor: All other contractors will avoid (to avoid the risk of complete dependence on a direct competitor), inhibiting sharing
- **OSS development:** First-mover advantage
 - First one to release defines architecture & has best expertise in the OSS component, leading to competitive advantage

HOST Program

Closing government cybersecurity gaps by sponsoring open source projects

- Suricata Intrusions Detection System
- OpenSSL FIPS validation

...and helping government be able to find and deploy existing open source cybersecurity solutions

- Inventory of solutions, **opencybersecurity.org**
- Use cases & lessons learned reports
- Improved policy

Open Information Security Foundation - Suricata

- A new model for managing and sustaining innovation
 - A non-profit to develop and “own” the code
 - Software Freedom Law Center created the License pro bono
 - A consortium of companies providing support in exchange for not having to release changes
- Ground-up rewrite
 - Multi-Threaded
 - Automated Protocol Detection
 - File Identification and Extraction
 - GPU Acceleration



~\$1.2m in DHS funding was matched by ~\$8m in commercial sponsorship

How we can work together

- Include your open source efforts in our inventory
 - Projects owners maintain small .xml, we crawl for updates
- Let us know of projects that Gov should be using
- Let us know if there are some successes that would make a good case study
- Do you want to take your work Open Source...
 - We can help!
- Having trouble finding OS to build on top of?
 - We can help with that too!