APPENDIX E

FOSS SECURITY ISSUES

1. The importance of security

Whereas organisations have to consider many factors when implementing information systems in software, including flexibility, features, scalability and cost, security is a paramount concern for government. Information systems that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system. The state has a strong obligation to its citizens that it does not compromise in these areas.

2. Countering false perceptions

The perception that FOSS is less secure than "professionally" developed closed-source proprietary software is a common one, but is substantially flawed. As many governments are concluding, including most of the governments of the European Union (who are almost all considering greater FOSS deployment), the security argument in favour of FOSS is a strong one.

> *Gartner analyst John Pescatore says that many open source solutions are actually more secure than closed source solutions and thus may even be a better fit in the government sector.*
>
> *"There is a myth out there that because the bad guys see the code, there are more vulnerabilities," Pescatore said. "But the truth is that the better predictor of robust code is whether security was a top priority during the development cycle or just an afterthought." In his opinion, the security argument against open source is a dead issue.*
>
> (quoted in TechTarget, April 2006,

http://searchopensource.techtarget.com/originalContent/0,289142,sid39_gci1180306,00.html)

3. National security as a driver

Indeed the potential of more secure systems, and the ability to draw upon peer-reviewed verification of that security, is frequently a major driver in the adoption of FOSS by governments. The benefit FOSS can have of removing dependency on a single vendor, has substantial implications for security. Many countries are seeing the potential FOSS offers to re-assert national self determination in the field of information systems. The

most compelling recent example of such thinking comes from an increasingly influential China:

> *... Ni Guangnan, an academician at the Chinese Academy of Engineering, who also expressed a similar opinion of "taking our fate into our own hands." Ni says that China is promoting open source as part of its strategy of being an innovative country, for national information security, and to solve the software pirate problem*"
>
> (quoted in Newsforge, September 2006,

http://business.newsforge.com/article.pl?sid=06/09/18/1835233)

Even in the absence of policy, it is common to find existing FOSS deployment in the more security sensitive systems of government. The South African government itself has deployed FOSS firewalls and gateways to protect the government common core network for more than ten years. Other notable examples include FOSS deployment by the US Navy and the French Police Service. In these areas, where information security skills are often the most developed, FOSS solutions have long been the natural choice of security experts.

4. Rising to the challenge

It is important not to make naïve assertions in the area of national information systems. This policy is not suggesting that any or all FOSS applications downloaded from the internet are by their nature secure and suitable for deployment everywhere. But South African government experience, as well as that of others, is increasingly leading us to conclude that the informed deployment of FOSS, in appropriate partnership with vendors where necessary, will result in more secure systems over which we exert greater national control. And the more we are able to develop our FOSS security skills base the more we will be able to reap these security benefits of FOSS. This should be seen as an enormous opportunity and national priority rather than a barrier to adoption.