File 20090608.1026: Ronal Kainda from reading group and STX wants to send me email about something. Notes from reading through NISP SP 800-53 revision 3:

- NIST responsibilities under FISMA for federal IS except for national security systems
- Also consistent with OMB circular A-130
- FISMA→FIPS 200 (mandatory standard)
- FIPS 199 defines the categories; then 800-53 provides a catalogue of controls.
- Question: what is the one that will replace DCID 6/3? Answer: it is NIST SP 800-53 revision 3, when it gets approved. This is from the guys at AFRL during the Prob. Redaction kickoff meeting in March 2009. They said that when SP 800-53 gets approved, DCID 6/3 is dead.
- Quote: 'The answers to these questions were not given in isolation but rather in the context of an effective *information security programme* for the organisation that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks arising from its information and information systems.' [2, p. 1]
- 44 U.S.C., §3542 defines national security systems.
- SP 800-53 process:
  - **Categorise** the IS based on FIPS 199
  - **Select baseline** security controls
  - **Implement** security controls
  - **Assess** security controls
  - **Authorise** operation based on a determination of risk
  - **Monitor** security controls on an ongoing basis
- Definitions:

  low impact system In a **low impact system** all of C-I-A are *low*.

  moderate impact system In a **moderate impact system** at least one of the security objectives is *moderate*, and none is greater than moderate.

  high impact In a **high impact system** at least one security objective is *high*.

How to include `pic2plot` figures in LaTeX:

1. Put the `pic` source code in a file in `./graphics/` like this:

```
.PS
Work: box rad 0.1 "work";
move to Work .e
line up right dashed;
School: ellipse "school";
move to School .e
line down right dashed;
ISSEP: box rad 0.1 "ISSEP";
move to ISSEP .w;
line left to Work .e;
line down right dotted;
Home: box "home";
move to Home .n;
line to School .s dotted;
.PE
```

2. Then convert it to a format that LaTeX can use like this:

```
% pic2plot school-work-home.pic | plot -T ps > school-work-home.ps
% ps2pdf school-work-home.ps
% mv school-work-home.pdf graphics
% rm school-work-home.ps
```

3. The result looks like Figure 1.

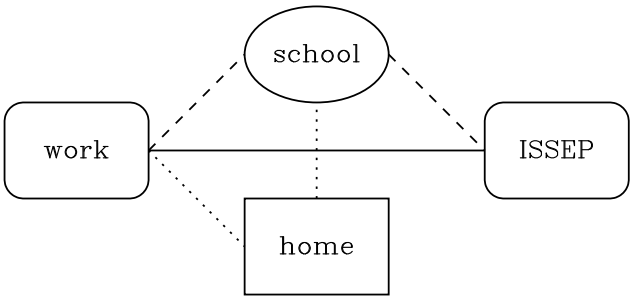

Figure 1: Relationship between school, work, home, and the ISSEP examination.

The reference for `pic` is in [1].

More quotes from NIST SP 800-53 revision 3:

- 'In selecting the security controls and control enhancements to supplement the tailored baseline, an organisation can employ a *requirements definition* approach or a *gap analysis* approach.' [2, p. 23]
- 'For a new development system, the security control selection process is applied from a *requirements definition* perspective since the information system does not yet exist and the organisation is conducting an initial security categorisation.' [2, p. 24]
- 'In contrast, for a legacy information system, the security control selection process is applied from a *gap analysis* perspective when the organisation is anticipating significant changes to the system (e.g., during major upgrades, modification, or outsourcing).' [2, p. 24]
- 'The first security control in each family (a.k.a. the *dash one* control) generates the requirement for policy and procedures. . . ' [2, p. F-2]

References

[1] Eric S. Raymond. *Making Pictures with GNU PIC*. `eric@snark.thyrsus.com`, unknown year.

[2] U.S. Department of Commerce, National Institute of Standards and Technology. *NIST Special Publication 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations*, June 2009. Final Public Draft.