



# RT for Incident Response (RTIR)

Andy Bone

JANET-CERT Manager



## JANET-CERT

Migrating to new version [RT 3.2.1 / RTIR 1.2]  
Is looking into removing spam/rejected from db, awaiting answer from Bestpractical, building a new GPG module.

## REDIRIS

No update, still using, will evaluate new version.

## SWITCH

Still no production RTIR  
Needs more flexible ACL's  
Has a multi-constituency model as proof of concept  
Would like to be able to close incidents without creating incident report etc



## ACONET

Testing new version  
Spam is a major problem

## SURFNET

Still evaluating

## CERT POLSKA

Has used RTIR in production for over a year.  
Has increased performance by restarting db



## SUNET-CERT

Has been using RT for 4 years

Still evaluating RTIR

Has many old RT tickets, would need easy import method

## GOVCERT-NL

Evaluating



## 11.2/08 [RTFM + advisories]

- No problems integrating and almost zero cost
- JANET-CERT will write requirement.

## 11.2/12 [access to rt queues]

- Ongoing, no news
- Closing incidents without creating incident report
- ACONet CERT to write requirement

## 11.2/13 [improved upgrade procedures]

- Included in new build
- Will ask for rubbish delete/archive in next build
- JANET-CERT to write requirement.



## 11.2/14 [automatic report generator]

- JANET-CERT to send around the JANET classifications.
- JANET-CERT will investigate further and post to m/list.

## 22.4/01 [Code of Practice]

- JANET-CERT will distribute for discussion
- Comments by end of 1st week in October

## 22.4/02 [TERENA Contractual Issues]

- Ongoing, will contact TERENA when new requirements are drawn up



## 22.4/04 [GPG]

- Ongoing, CFB building new module
- Requirement will be written by CERT-PL and JANET-CERT

## 22.4/05 [DTD]

- Carlos has a working XML output but wants to improve the DTD
- CFB will send current DTD to mailing list
- Requirement will be written by JANET-CERT

## 22.4/06 [PH's paper on Multi Constituencies]

- Peter will redistribute
- Comments by end of 1st week of October
- Requirement will be written by Switch-CERT



## 22.4/07 [Template Plug in]

- Will be completed after Malta
- SWITCH-CERT will write requirement

## 22.4/08 [Multiple 'investigation to:']

- Andy to chase Bestpractical regarding John's patch, included into next build



First submissions for requirements by the beginning of November

Andy to source venue for 1day RTIR meeting in London (maybe Didcot)

JANUARY 2005, TF-CSIRT, LONDON (with a possible video conference in between)

# Finding out more



[rtir-request@lists.bestpractical.com](mailto:rtir-request@lists.bestpractical.com)

- Closed list for incident response team staff

<http://www.bestpractical.com>

<http://www.bestpractical.com/pub/rt/release/rtir.tgz>

[sales@bestpractical.com](mailto:sales@bestpractical.com)

# Questions

