

***Vulnerability and Exploit
Description and Exchange
Format (VEDEF)
TF-CSIRT Progress Update***

Dave Freeman
*(representing Ian Bryant,
VEDEF WG Co-Chair)*
24th September 2004

Contents









- Summary of Activities
- Proposed Flow Model
- Details of Profiles
- Way Ahead
- Questions ?

Activities since May TF-CSIRT

- Briefing to FIRST Birds of Feather session, Budapest June 2004 :
 - Broadly supportive
- Briefings to IETF :
 - Interim INCH meeting, Budapest June 2004, broadly supportive
 - IETF60 (San Diego August 2004) INCH meeting had little support
- Alternative way ahead road-mapped with CERT/CC and JPCERT/CC

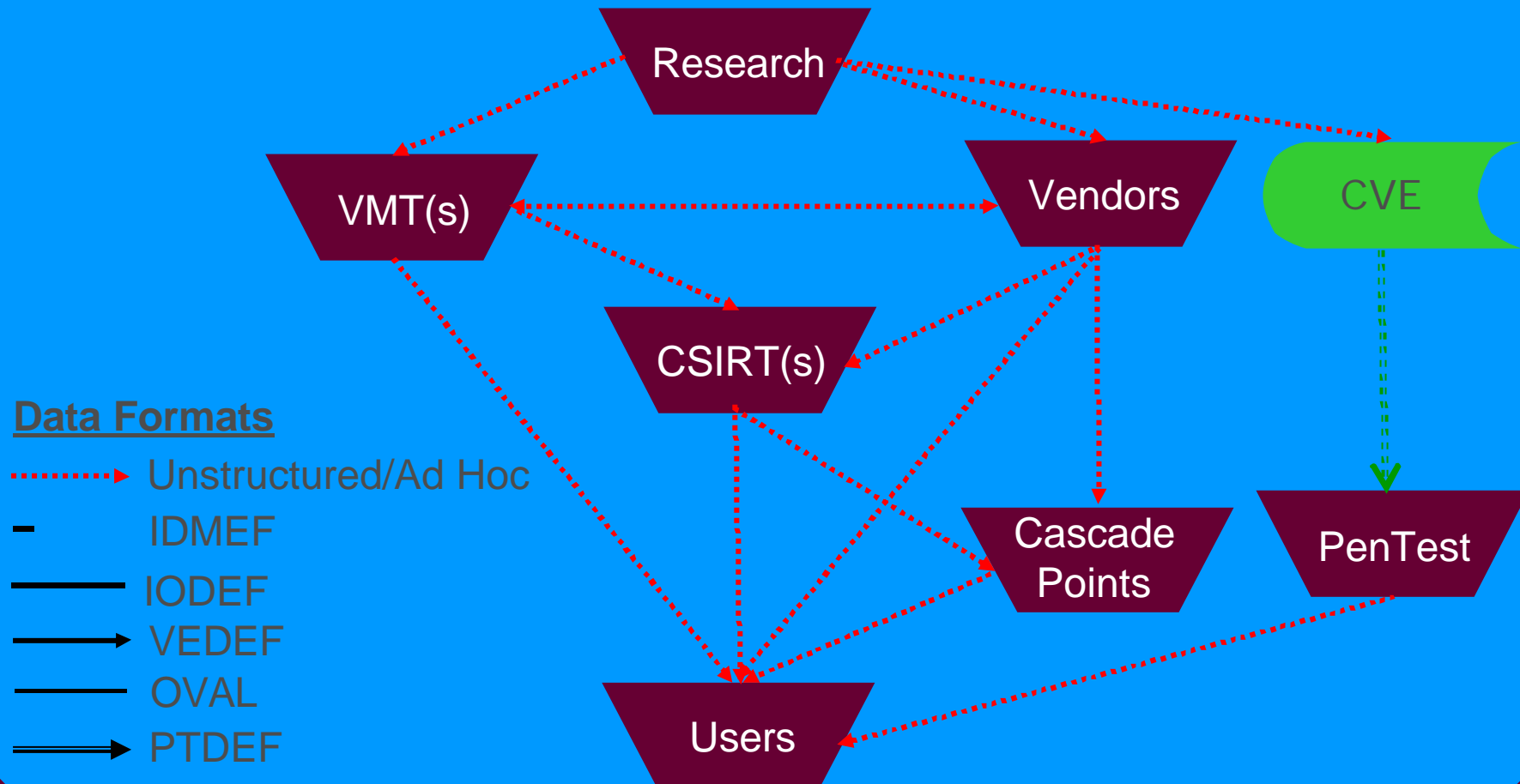
Colour Code and Acronyms

Data / Storage Formats

	No Standard	
	Concept Only	
	Pilot(s) in use	
	Standard Exists	

- CSIRT – Computer Security Incident Response Team
- CVE – Mitre database format
- DEF – Description and Exchange Format
- IDMEF – Intrusion Detection Management Exchange Format
- IODEF – Incident Object DEF
- OVAL – Mitre data format
- PTDEF – Penetration Test DEF
- RT – Request Tracker software
- RTIR – RT for Incident Response
- RTPT – RT for Penetration Test results
- RTVE – RT for Vulnerabilities and Exploits
- VEDEF – Vulnerability and Exploit DEF
- VMT – Vulnerability Management Team

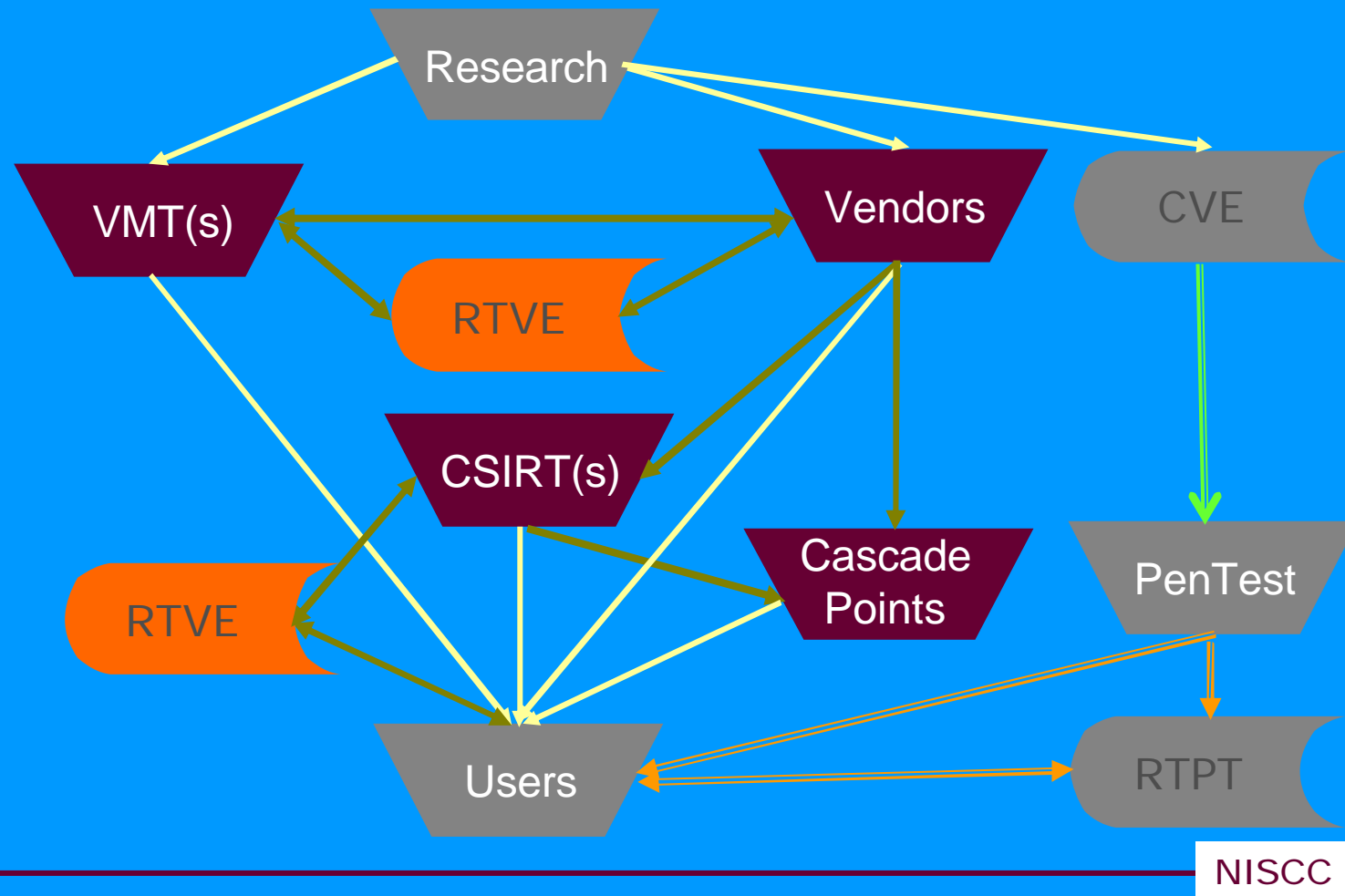
Current Vulnerability Information Flow



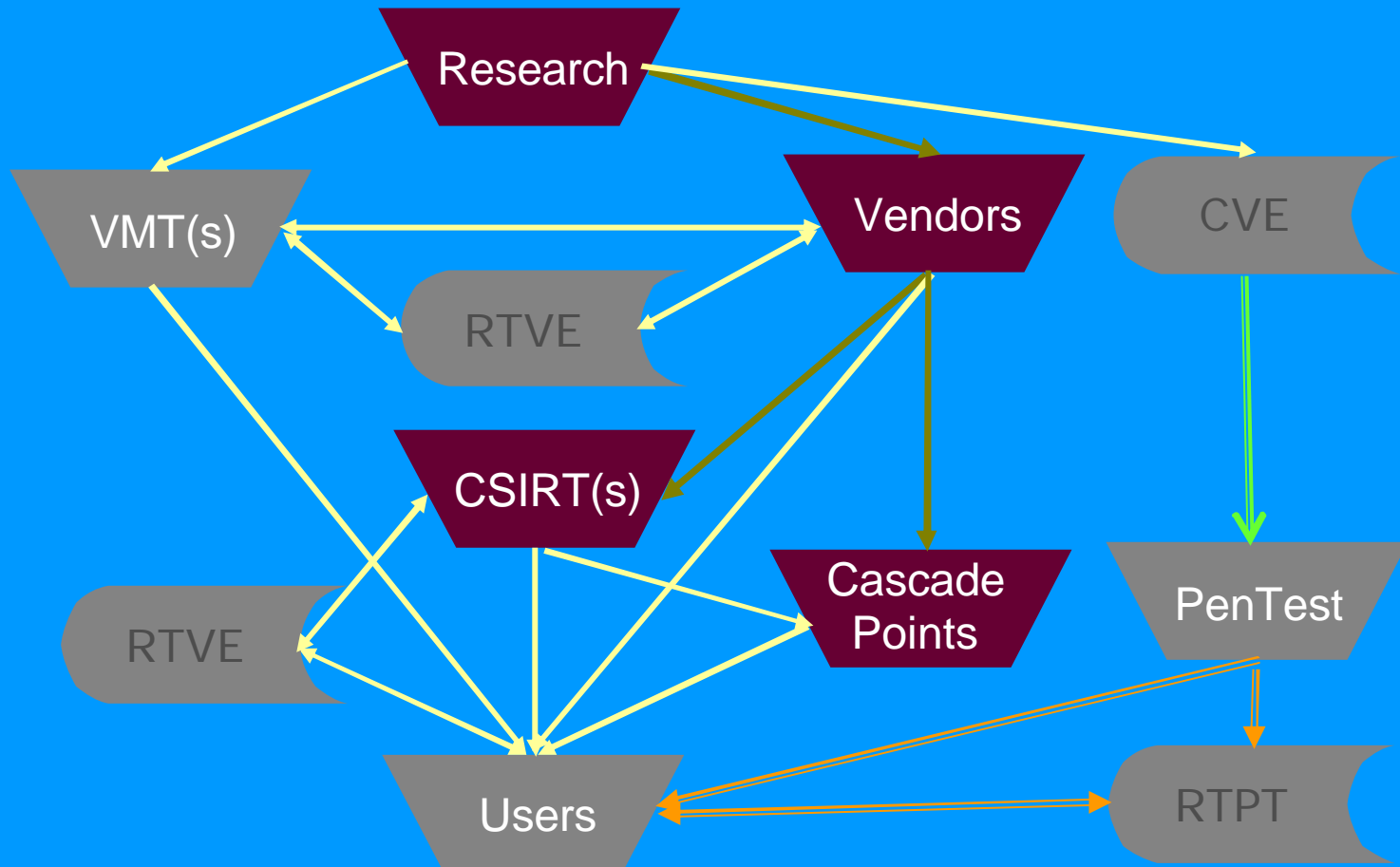
Vulnerability Information Flows: The Need for Profiles

- VEDEF envisaged as a Superset of the information required
- Various subsets (“Profiles”) needed to support user Communities of Interest
 - Vulnerability Management
 - Vendors
 - Technical Dissemination
 - Plain-Language Dissemination

Proposed Flow Vulnerability Management Profile

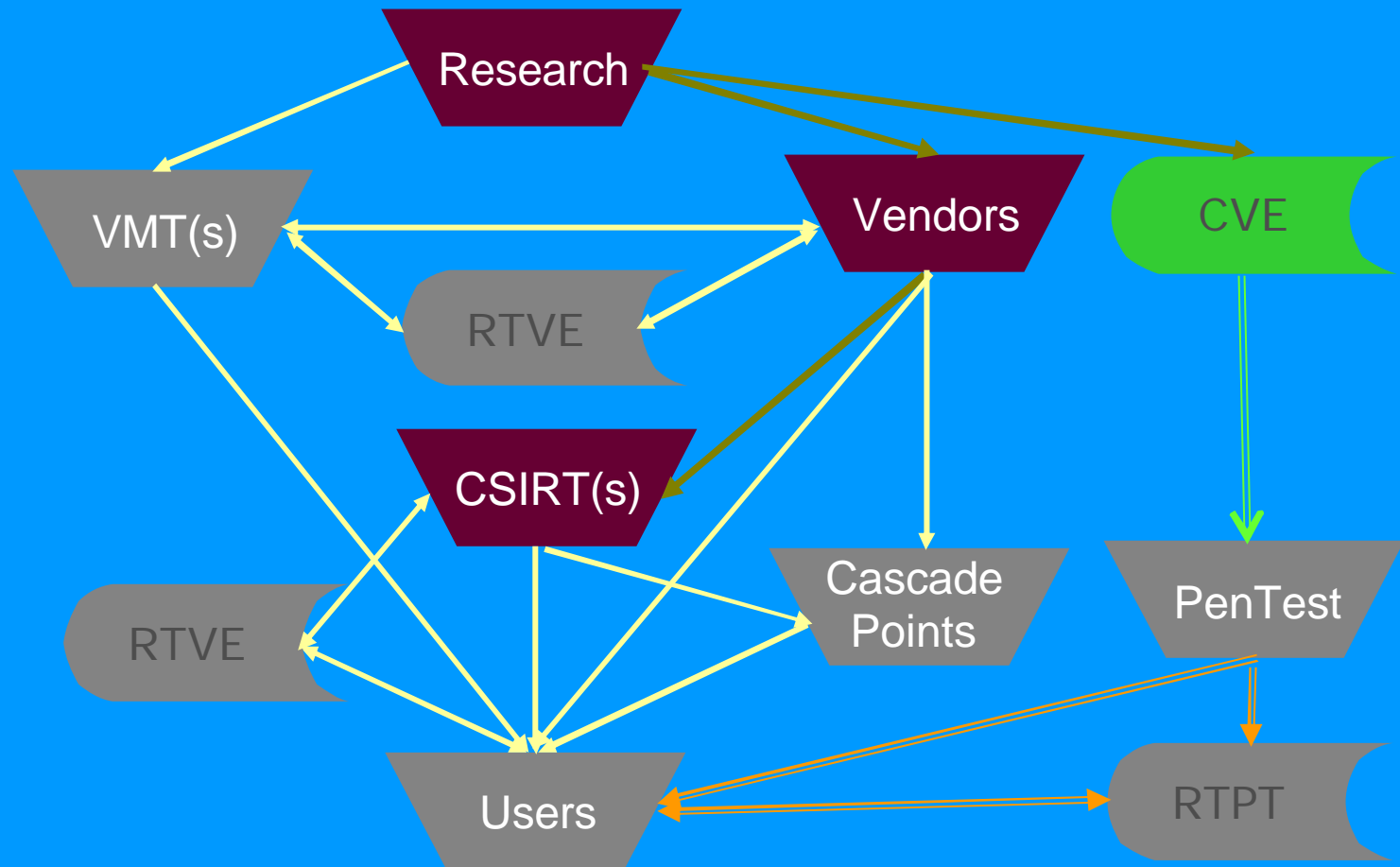


Proposed Flow Vendor Profile



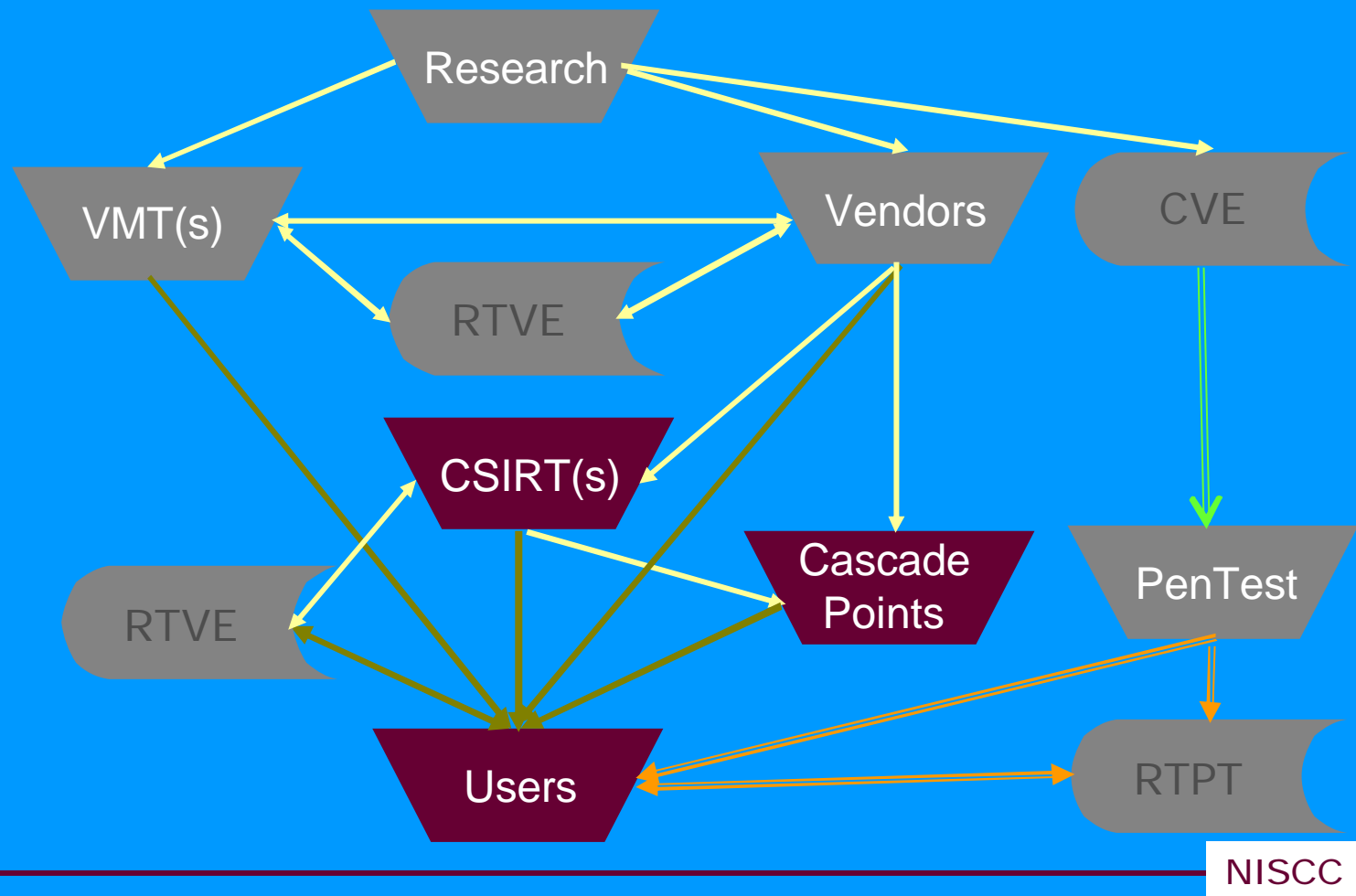
NISCC

Proposed Flow Technical Dissemination Profile



NISCC

Proposed Flow Plain Language Alert Profile



VEDEF Profiles: Summary of Unique Elements

VEDEF will consist of a common core of XML data for all uses, with additions to support:

- Vulnerability Management Profile
 - Handling restrictions e.g. Embargo Dates, Shareability
- Vendor Profile
 - e.g. Vendor-specific Version-strings and Scripts
- Technical Dissemination Profile
 - Generic Risk Assessment for CSIRT's own community
- Plain-Language Dissemination
 - "Grandparent-friendly" what-to-do advice

Proposed Way Ahead

- VEDEF jointly developed by TF-CSIRT and JPCERT/CC
 - Still need to gain support of others
 - W3C
 - Expanded Vendor base
- Produce series of IETF RFCs as “Individual Contributions”
 - Informational or Experimental RFC don't need sponsor WG
 - Consider Birds of Feather (BOF) at IETFs for visibility
- Main Working Channel will be via Mailing Lists
 - TF-CSIRT internal
 - Open (<http://www.vedef.org/contact.html>)

Questions?



Contact Details

NISCC Capability Development Group VEDEF Project Team

PO Box 832, London, SW1P 1BG, England

Telephone: +44-87-0114-4568; Dave Freeman
+44-87-0114-4561; Ian Bryant

Facsimile : +44-20-7821-1686

Internet

ibryant@vedef.org
dfreeman@vedef.org

<http://www.vedef.org>