

# ***Vulnerability and Exploit Description and Exchange Format (VEDEF) - Situation Report***

Ian Bryant  
Head of *ITsafe* Service  
& TF-CSIRT WG Chair

13<sup>th</sup> May 2005  
*TF-CSIRT Zürich*

TF-CSIRT  
VEDEF WG

# Topics

---

- How did we get here?
- Cooperation and Deconfliction
- Proposed Way Ahead
- Questions ?

# Topics

---

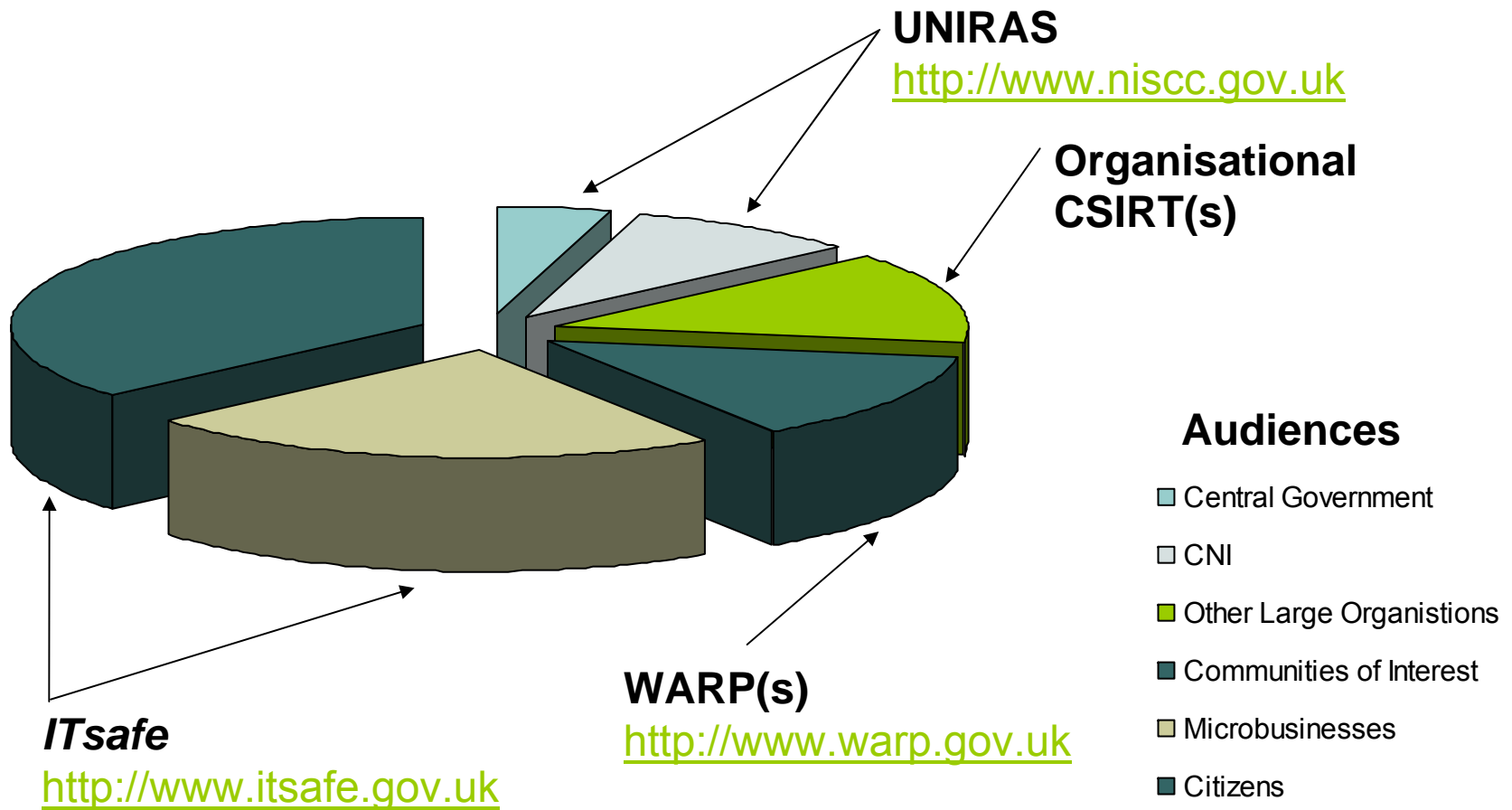
- ▶ How did we get here?
- Cooperation and Deconfliction
- Proposed Way Ahead
- Questions ?

# Vulnerability and Exploit Description and Exchange Format (VEDEF)

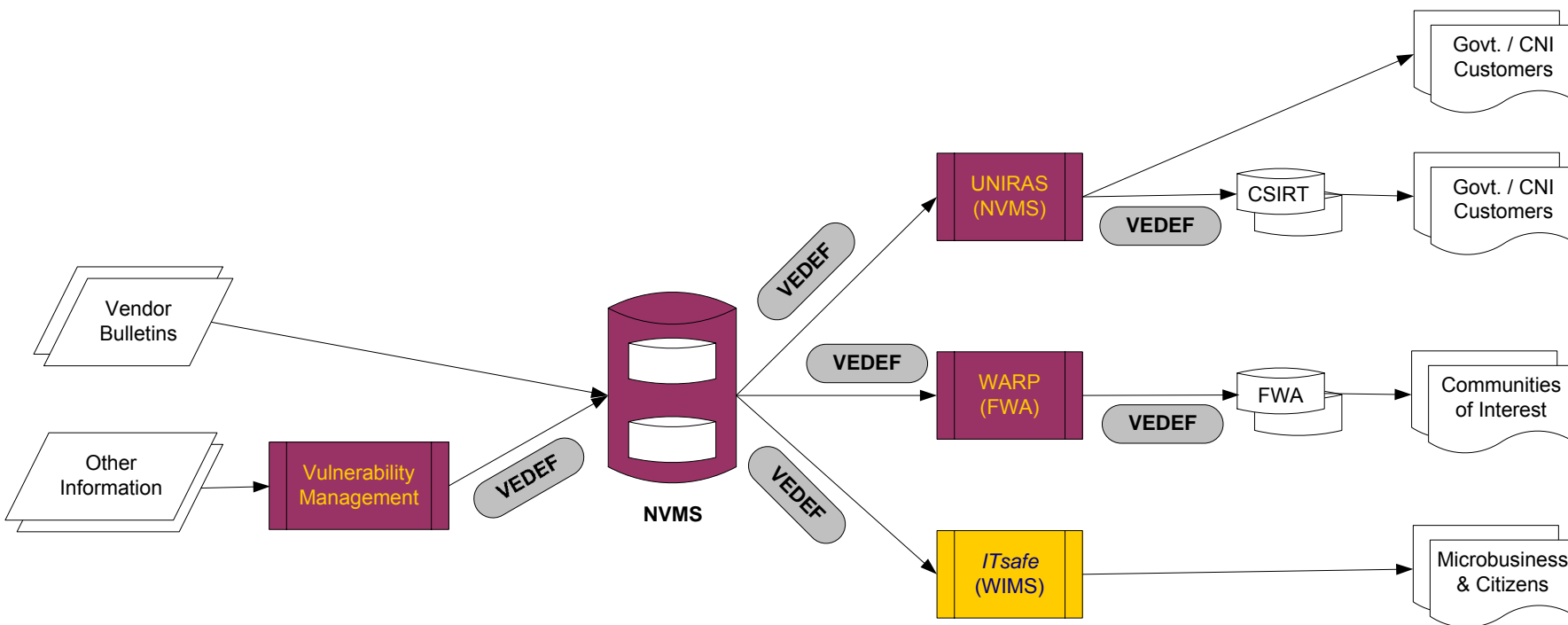
---

- The *de facto* standard for storage of Vulnerability information is Mitre's Common Vulnerabilities and Exposures (CVE)
- This does not seem to meet the needs of the CSIRT community for Information Exchange
- There are (at least) 5 existing initiatives (EISPP, CAIF, OpenSec, ANML, VulDef) :
  - Varying degrees of activity in their development
  - Being proposed by differing regions / communities
  - No historic efforts towards their deconfliction
- The concept of a Vulnerability and Exploit DEF (VEDEF) was therefore needed

# Example of VEDEF Requirement - NISCC Multiple Output Formats (1)



# Example of VEDEF Requirement - NI SCC Multiple Output Formats (2)



## **VEDEF - Basic Information Requirement**

---

- Description of the platform(s) affected
- Description of the nature of the problem
- Description of the likely impact if the Vulnerability and/or Exploit were, accidentally or maliciously, triggered
- Available means of remediation
- Disclosure restrictions

# VEDEF Information Flows - The Need for Profiles

---

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
  - Citizen and SME orientated "what-to-do" advice

# TF-CSIRT VEDEF Working Group Charter

---

Produce a series of documents establishing consolidated Best Practice for Vulnerability and/or Exploit description

- Functional requirements of data format for collaboration between Vendors, CSIRTs and end users
- Specification of the extensible, data language to describes the data formats to satisfy the requirements
- Guidelines for implementing the WG data format, with a set of sample Vulnerability and/or Exploit reports and their associate representation in the data language

# Topics

---

- How did we get here?
- ▶ Cooperation and Deconfliction
- Proposed Way Ahead
- Questions ?

# VEDEF - Relationship to other Initiatives

---

- In active discussion with VEDEF WG:
  - CAIF
  - EISPP incl. CAF and CMSI
  - VULDef (JPCERT/CC)
- Need to consider linkages to:
  - CVE
  - CVSS
  - OVAL
  - VDF

# Topics

---

- How did we get here?
- Cooperation and Deconfliction
- ▶ Proposed Way Ahead
- Questions ?

# VEDEF - Proposed Way Ahead

---

- VEDEF WG (including EISPP members and CAIF) develop converged Existence Proof with JPCERT/CC (VULDef)
  - Still need to work on deconfliction with other Initiatives
  - Provide Birds of Feather (BOF) session at FIRST Conference
  - Investigate linkages to ENISA Work Programme
- Main Working Channel will be via Mailing Lists
  - TF-CSIRT internal
  - Open (<http://www.vedef.org/contact.html>)
- Ultimately submit outputs to IETF as (Informational or Experimental) RFCs using “Individual Contribution” procedures
  - Don’t need sponsor WG (problems with INCH in past)
  - Consider interim BOF(s) at IETFs for visibility

# Questions?

---



# Contact Details

---

## *NISCC Capability Development Group*

PO Box 832, London, SW1P 1BG, England

Telephone: +44-87-0114-4561; Ian Bryant  
+44-87-0114-4546; Dave Freeman  
Facsimile : +44-87-0487-0749

### Internet

[ibryant@vedef.org](mailto:ibryant@vedef.org)

[dfreeman@vedef.org](mailto:dfreeman@vedef.org)

<http://www.vedef.org>

[csirt-vedef@terena.nl](mailto:csirt-vedef@terena.nl) (unmoderated)