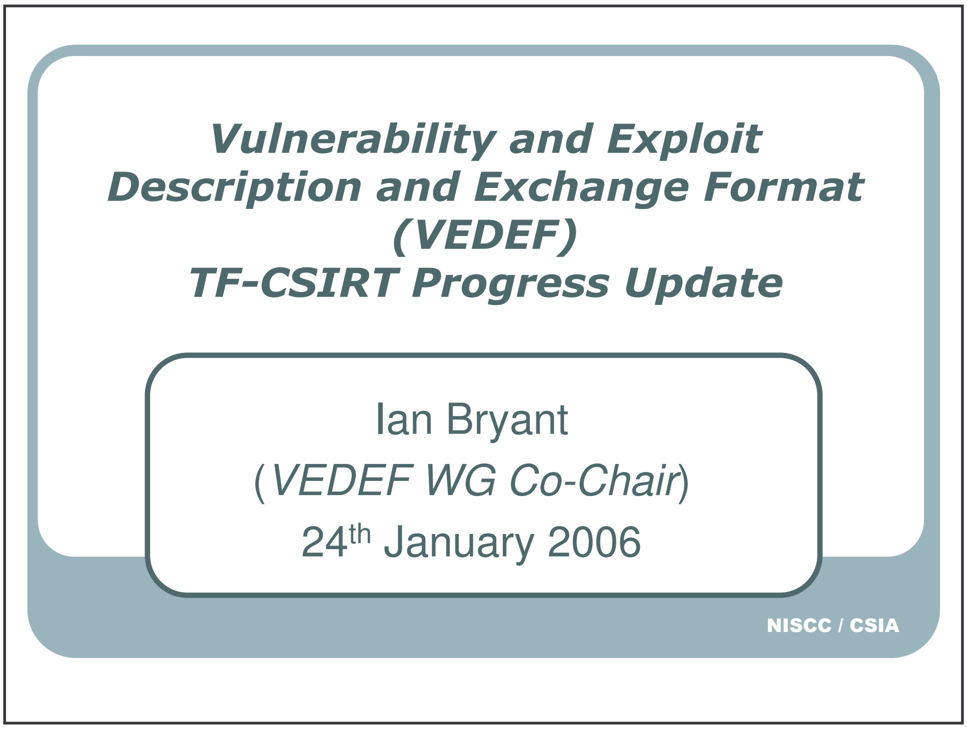


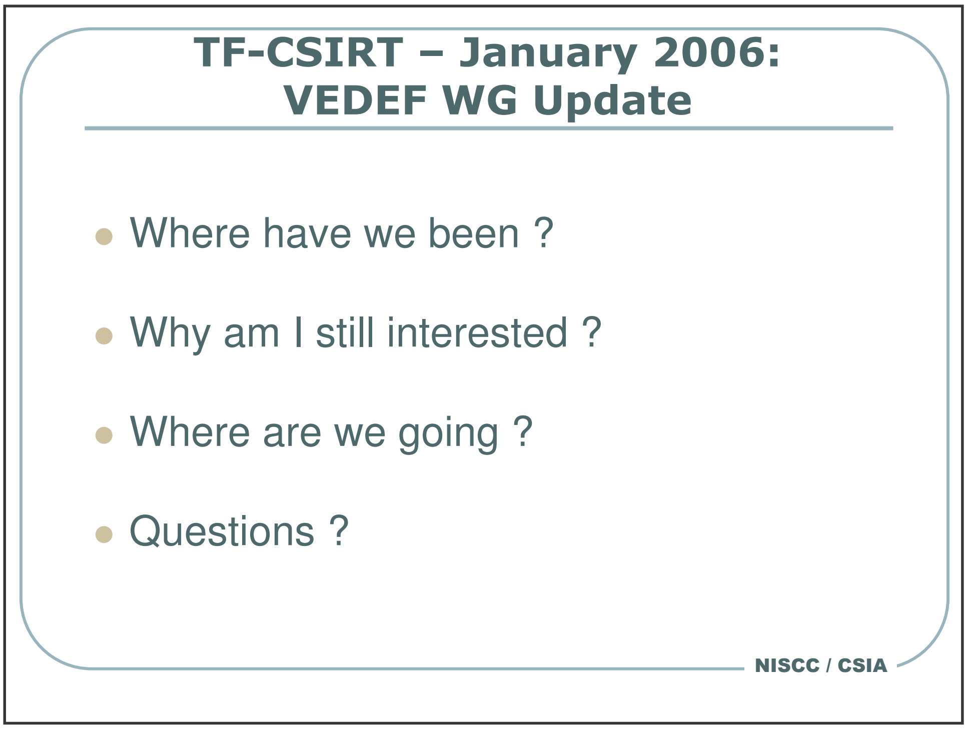
Vulnerability and Exploit Description and Exchange Format (VEDEF) TF-CSIRT Progress Update

Ian Bryant

(*VEDEF WG Co-Chair*)

24th January 2006

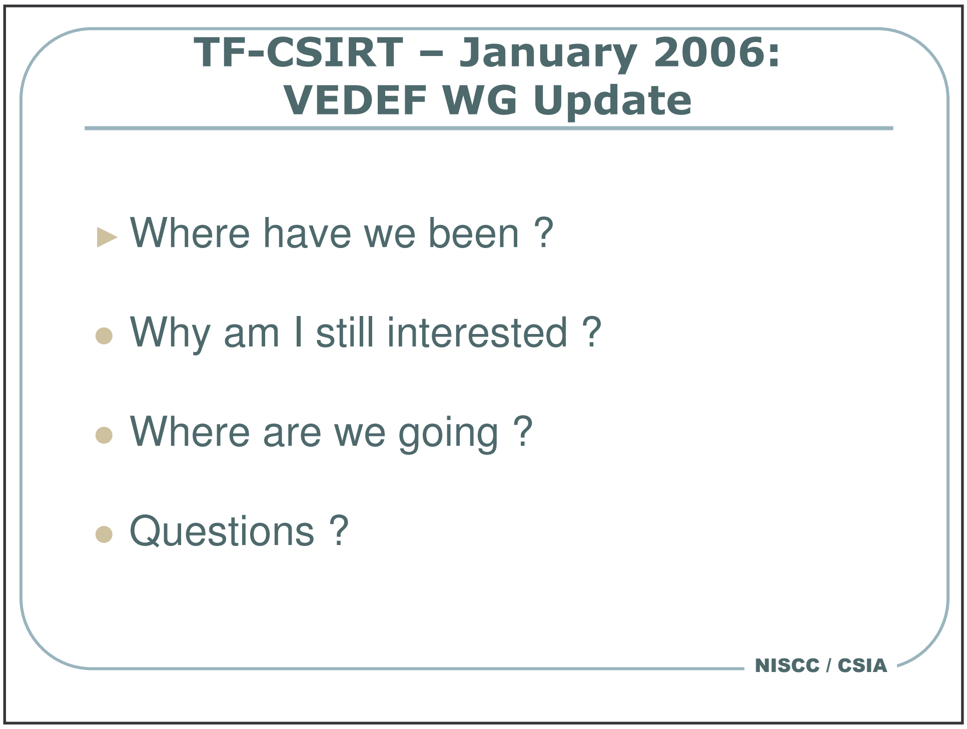
NISCC / CSIA



TF-CSIRT – January 2006: VEDEF WG Update

- Where have we been ?
- Why am I still interested ?
- Where are we going ?
- Questions ?

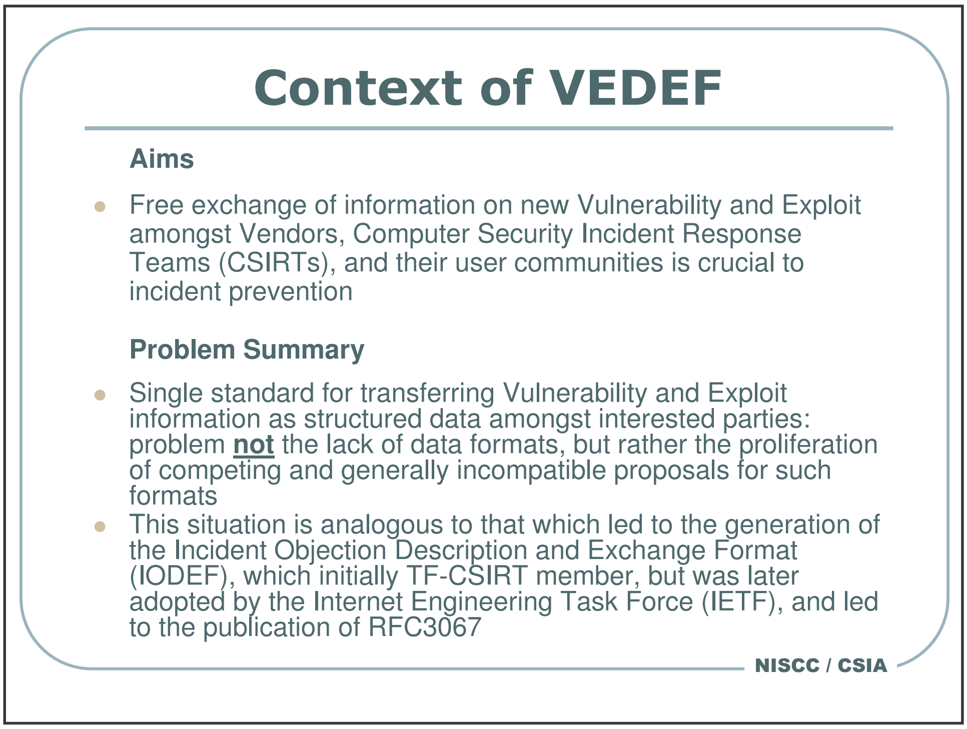
NISCC / CSIA



TF-CSIRT – January 2006: VEDEF WG Update

- Where have we been ?
- Why am I still interested ?
- Where are we going ?
- Questions ?

NISCC / CSIA



Context of VEDEF

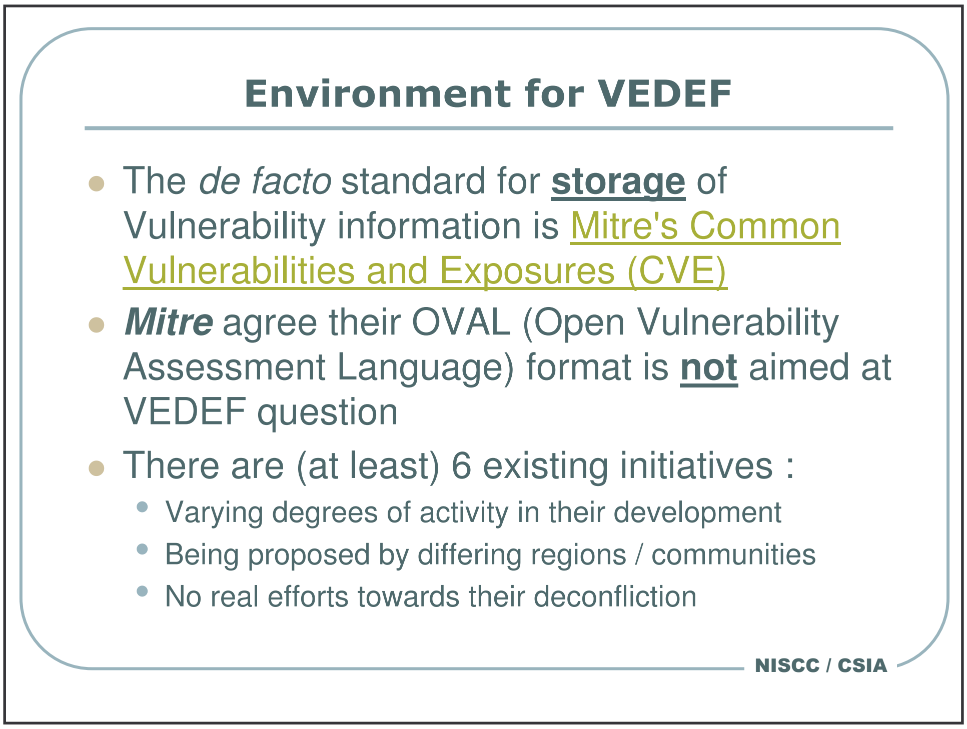
Aims

- Free exchange of information on new Vulnerability and Exploit amongst Vendors, Computer Security Incident Response Teams (CSIRTs), and their user communities is crucial to incident prevention

Problem Summary

- Single standard for transferring Vulnerability and Exploit information as structured data amongst interested parties: problem **not** the lack of data formats, but rather the proliferation of competing and generally incompatible proposals for such formats
- This situation is analogous to that which led to the generation of the Incident Objection Description and Exchange Format (IODEF), which initially TF-CSIRT member, but was later adopted by the Internet Engineering Task Force (IETF), and led to the publication of RFC3067

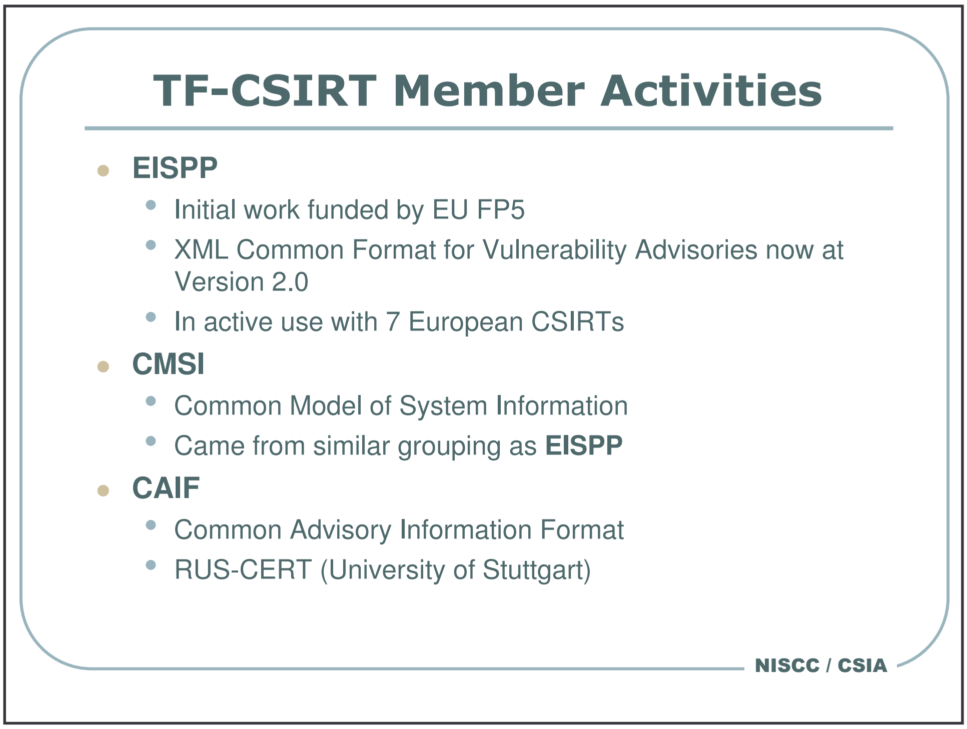
NISCC / CSIA



Environment for VEDEF

- The *de facto* standard for **storage** of Vulnerability information is Mitre's Common Vulnerabilities and Exposures (CVE)
- ***Mitre*** agree their OVAL (Open Vulnerability Assessment Language) format is **not** aimed at VEDEF question
- There are (at least) 6 existing initiatives :
  - Varying degrees of activity in their development
  - Being proposed by differing regions / communities
  - No real efforts towards their deconfliction

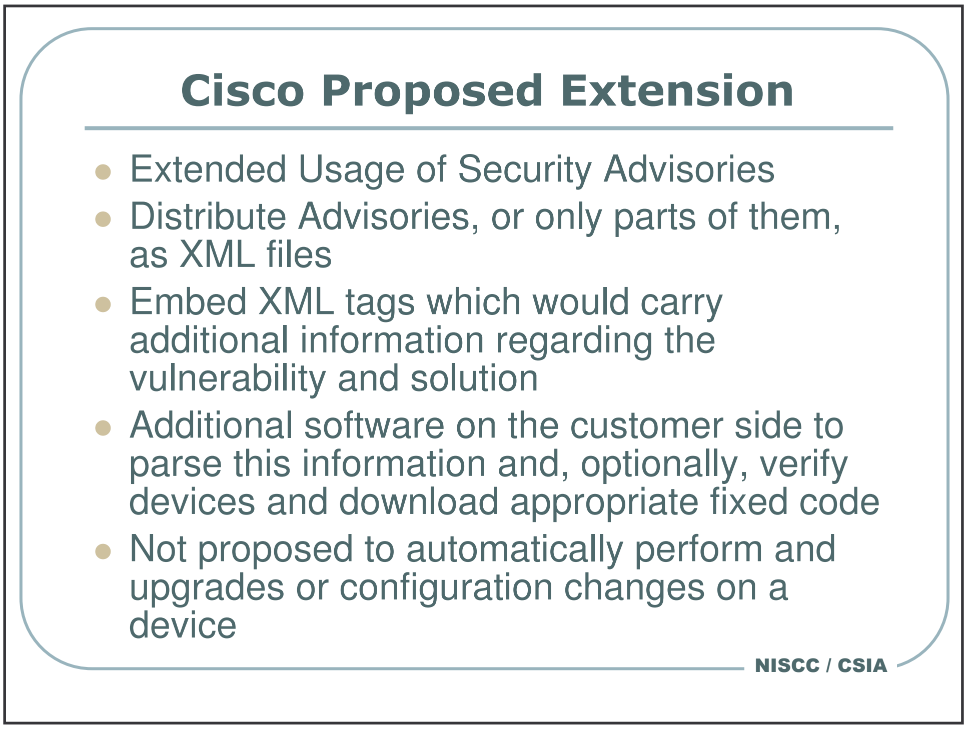
NISCC / CSIA



TF-CSIRT Member Activities

- **EISPP**
  - Initial work funded by EU FP5
  - XML Common Format for Vulnerability Advisories now at Version 2.0
  - In active use with 7 European CSIRTs
- **CMSI**
  - Common Model of System Information
  - Came from similar grouping as **EISPP**
- **CAIF**
  - Common Advisory Information Format
  - RUS-CERT (University of Stuttgart)

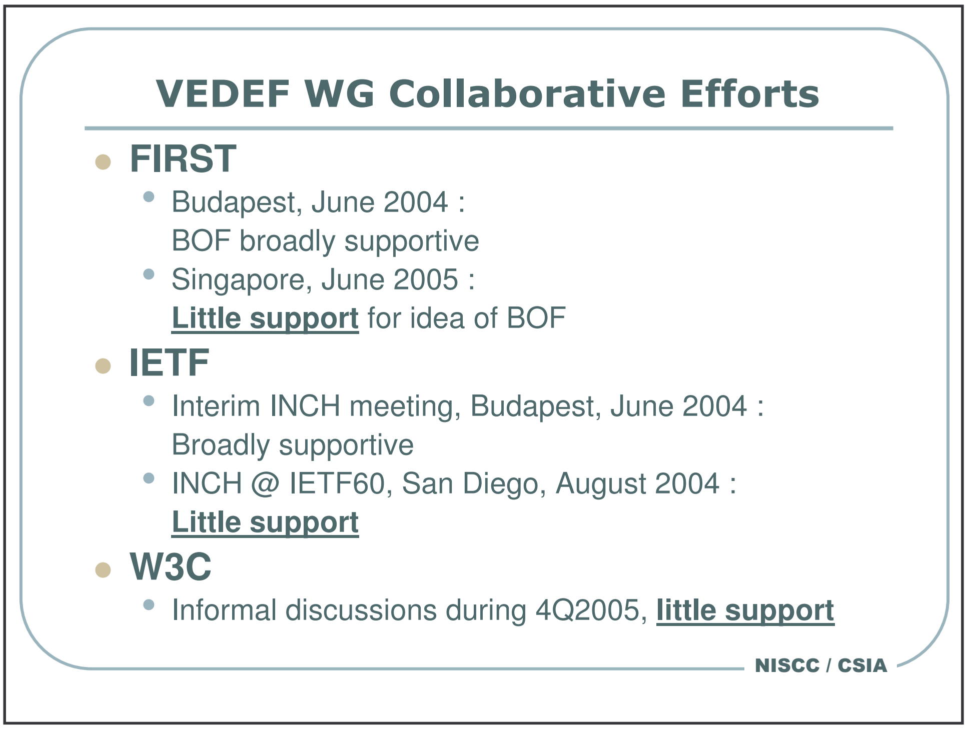
NISCC / CSIA



Cisco Proposed Extension

- Extended Usage of Security Advisories
- Distribute Advisories, or only parts of them, as XML files
- Embed XML tags which would carry additional information regarding the vulnerability and solution
- Additional software on the customer side to parse this information and, optionally, verify devices and download appropriate fixed code
- Not proposed to automatically perform and upgrades or configuration changes on a device

NISCC / CSIA



VEDEF WG Collaborative Efforts

- FIRST
  - Budapest, June 2004 :
    BOF broadly supportive
  - Singapore, June 2005 :
    Little support for idea of BOF
- IETF
  - Interim INCH meeting, Budapest, June 2004 :
    Broadly supportive
  - INCH @ IETF60, San Diego, August 2004 :
    Little support
- W3C
  - Informal discussions during 4Q2005, **little support**

NISCC / CSIA

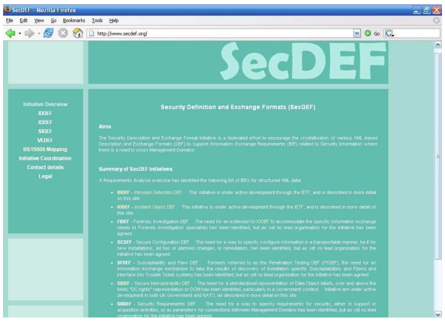
TF-CSIRT – January 2006: VEDEF WG Update

- Where have we been ?
- ▶ Why am I still interested ?
- Where are we going ?
- Questions ?

The SecDEF Initiative (1)

Security Description and Exchange Format

- A federated initiative to provide various XML based Description and Exchange Formats (DEF) to support security-related Information Exchange Requirements (IER) where there is a need to cross Management Domains
- A Requirements Analysis exercise has identified the following list of IERs for structured XML data:
  - IDDEF
  - IODEF
  - FIDEF
  - SCDEF
  - SFDEF
  - SIDEF
  - SRDEF
  - VEDEF
- `http://www.secdef.org`



Security Definition and Exchange Formats (SecDEF)

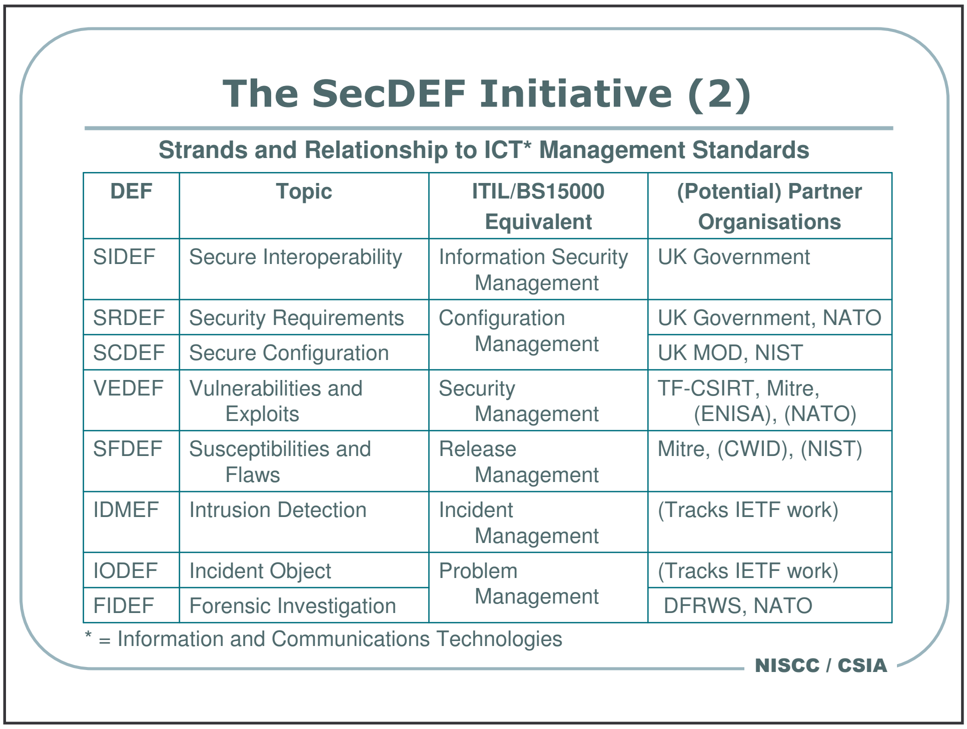
Aims

The Security Description and Exchange Format initiative is a federated effort to encourage the crystallisation of various XML based Description and Exchange Formats (DEF) to support Information Exchange Requirements (IER) related to Security Information where there is a need to cross Management Domains

Summary of SecDEF Initiatives

A Requirements Analysis exercise has identified the following list of IER's for structured XML data:

- **IDDEF** - Intrusion Detection DEF. This initiative is under active development through the IETF, and is described in more detail on this site
- **IODEF** - Incident Object DEF. This initiative is under active development through the IETF, and is described in more detail on this site
- **FIDEF** - Forensic Investigation DEF. The need for an extension to IODEF to accommodate the specific information exchange needs of Forensic Investigation specialists has been identified, but as yet no lead organisation for the initiative has been agreed
- **SCDEF** - Secure Configuration DEF. The need for a way to specify configure information in a transportable manner, be it for new installations, ad hoc or planned changes, or remediation, has been identified, but as yet no lead organisation for the initiative has been agreed
- **SFDEF** - Susceptability and Flaw DEF. Formerly referred to as the Penetration Testing DEF (PTDEF), the need for an information exchange mechanism to take the results of discovery of installation specific Susceptabilities and Flaws and interface into Trouble Ticket systems has been identified, but as yet no lead organisation for the initiative has been agreed
- **SIDEF** - Secure Interoperability DEF. The need for a standardised representation of Data Object labels, over and above the basic "DC rights" representation of DCMI has been identified, particularly in a Government context. Initiative are under active development in both UK Government and NATO, as described in more detail on this site
- **SRDEF** - Security Requirements DEF. The need for a way to specify requirements for security, either in support or acquisition activities, or as parameters for connections between Management Domains has been identified, but as yet no lead organisation for the initiative has been agreed



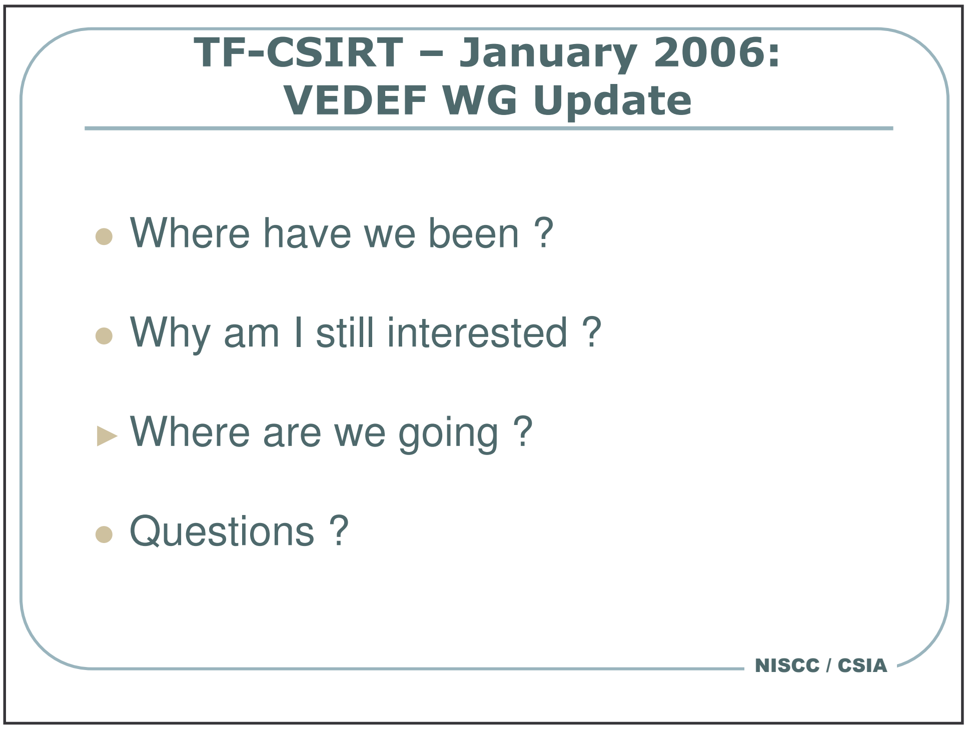
The SecDEF Initiative (2)

Strands and Relationship to ICT* Management Standards

DEF	Topic	ITIL/BS15000 Equivalent	(Potential) Partner Organisations
SIDEF	Secure Interoperability	Information Security Management	UK Government
SRDEF	Security Requirements	Configuration Management	UK Government, NATO
SCDEF	Secure Configuration		UK MOD, NIST
VEDEF	Vulnerabilities and Exploits	Security Management	TF-CSIRT, Mitre, (ENISA), (NATO)
SFDEF	Susceptibilities and Flaws	Release Management	Mitre, (CWID), (NIST)
IDMEF	Intrusion Detection	Incident Management	(Tracks IETF work)
IODEF	Incident Object	Problem Management	(Tracks IETF work)
FIDEF	Forensic Investigation		DFRWS, NATO

* = Information and Communications Technologies

NISCC / CSIA



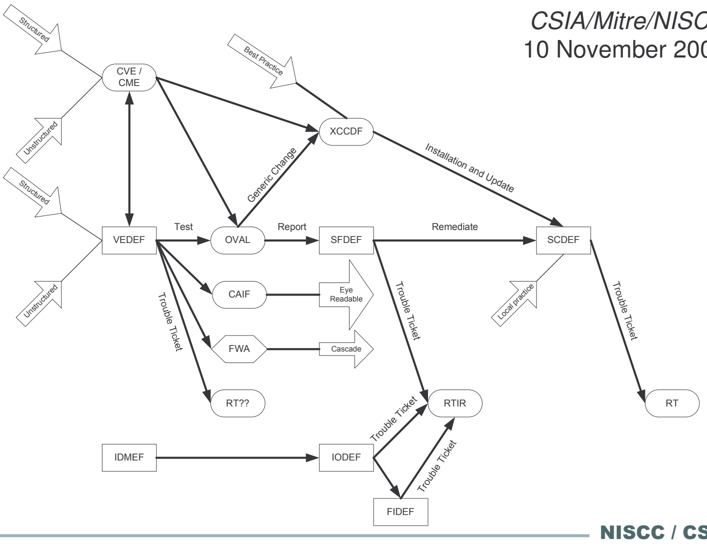
TF-CSIRT – January 2006: VEDEF WG Update

- Where have we been ?
- Why am I still interested ?
- ▶ Where are we going ?
- Questions ?

NISCC / CSIA

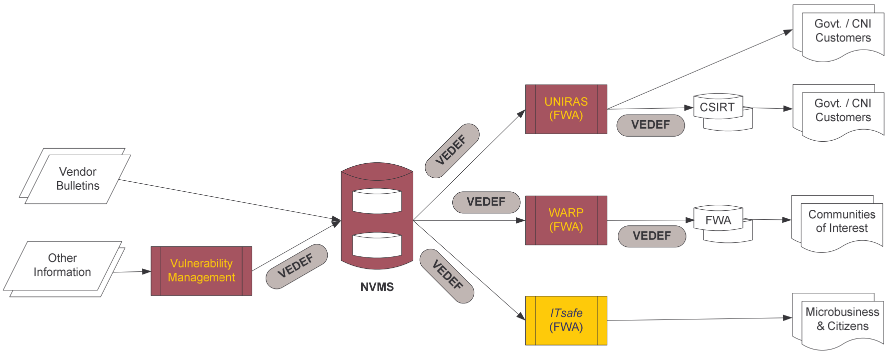
VEDEF – Evolutionary Context

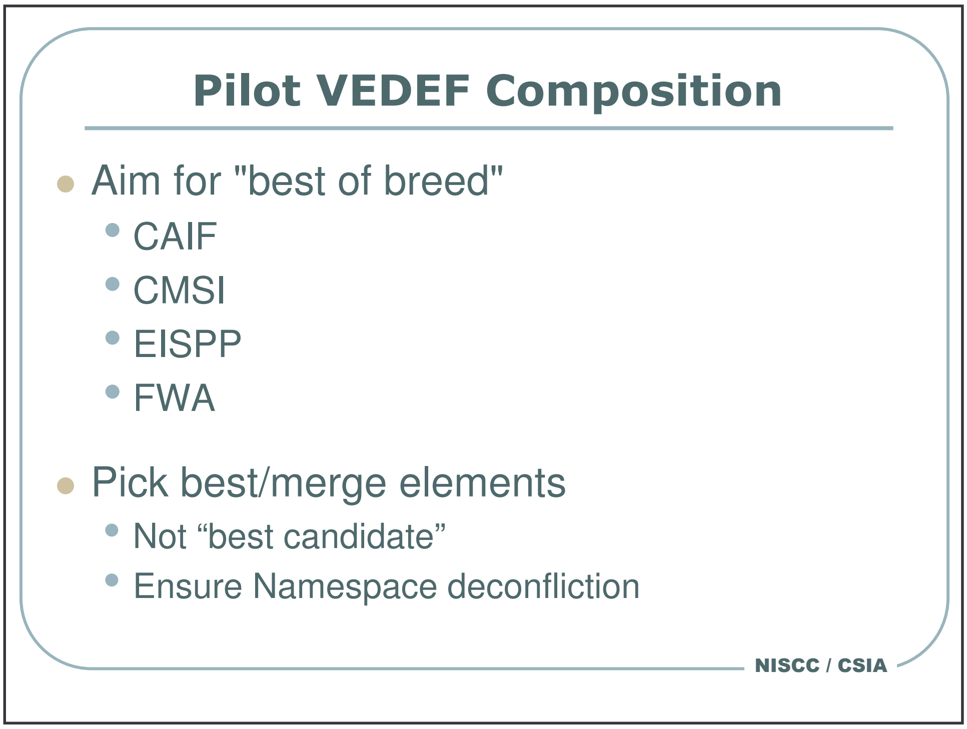
CSIA/Mitre/NISCC
10 November 2005



(Re-)Validation Pilot for VEDEF: Multiple Output Formats

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

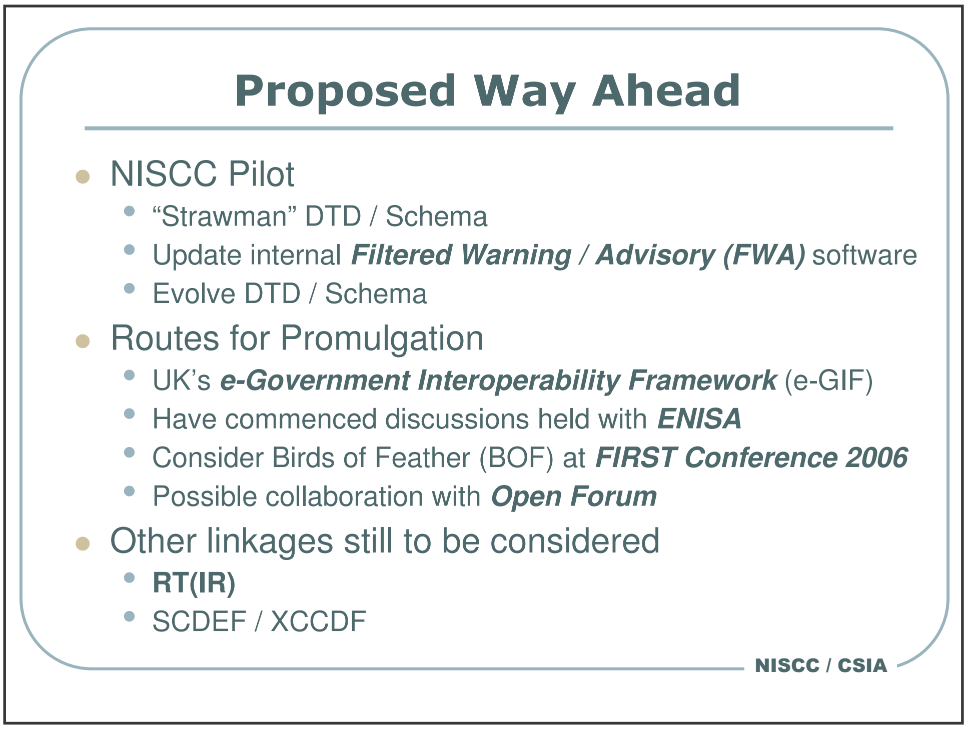




Pilot VEDEF Composition

- Aim for "best of breed"
  - CAIF
  - CMSI
  - EISPP
  - FWA
- Pick best/merge elements
  - Not “best candidate”
  - Ensure Namespace deconfliction

NISCC / CSIA



Proposed Way Ahead

- NISCC Pilot
  - “Strawman” DTD / Schema
  - Update internal ***Filtered Warning*** / ***Advisory (FWA)*** software
  - Evolve DTD / Schema
- Routes for Promulgation
  - UK’s ***e-Government Interoperability Framework*** (e-GIF)
  - Have commenced discussions held with ***ENISA***
  - Consider Birds of Feather (BOF) at ***FIRST Conference 2006***
  - Possible collaboration with ***Open Forum***
- Other linkages still to be considered
  - **RT(IR)**
  - SCDEF / XCCDF

NISCC / CSIA

Questions?

Contact Details

SecDEF Project Team
Capability Development Group

Central Sponsor for Information Assurance (CSIA)
Cabinet Office
6th Floor Stockley House
130 Wilton Road
London
SW1V 1LQ
England

Telephone: +44-87-0114-4561; Ian Bryant
+44-87-0114-4546; Dave Freeman
Facsimile : +44-20-7276-5096

Internet
ian.bryant@csia.gov.uk or david.freeman@csia.gov.uk
http://www.secdef.org